

PAT-NO: JP02000216774A
DOCUMENT- JP 2000216774 A
IDENTIFIER:
TITLE: CIPHER TEXT VERIFYING METHOD, RECORDING MEDIUM AND
DEVICE THEREOF

PUBN-DATE: August 4, 2000

INVENTOR-INFORMATION:

NAME	COUNTRY
ABE, MASAYUKI	N/A

ASSIGNEE-INFORMATION:

NAME	COUNTRY
NIPPON TELEGR & TELEPH CORP	N/A

APPL-NO: JP11015409

APPL-DATE: January 25, 1999

INT-CL (IPC): H04L009/32 , G09C001/00

ABSTRACT:

PROBLEM TO BE SOLVED: To verify the propriety of a cipher text without absolutely leaking information about a value in a verification expression by exponentiating a value calculated for verification, when **Cramer-Shoup** cryptograph is decoded by random numbers whose values are incapable for anyone to know trying to decode it and verifying whether or not the exponentiated result becomes 1.

SOLUTION: Although a cipher text prepared by a cipher text preparing device 11 is decoded by the device 12 of a decoding person, a device 13 of a verifying person verifies whether or not decoding rejection is appropriate so as to avoid rejecting decoding, because it is not a correct cipher text in a self-serving manner. After receiving a cipher text $E=(u_1, u_2, v, e)$ of a plaintext (m) enciphered by the **Cramer-Shoup** cryptograph method making X, Y and Z

public keys, the device 12 generates a random number (r) and calculates $(c)=H(u_1, u_2)$ and $(v)=(u_1X_1+CY_1u_2X_2+CY_2V_1)r \bmod (p)$. If (v) is 1, this cipher text is deemed accepted, but if (v) is not 1, it is deemed rejected, and the rejection is verified to a third person.

COPYRIGHT: (C)2000,JPO

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-216774

(43)Date of publication of application : 04.08.2000

(51)Int.Cl.

H04L 9/32
G09C 1/00

(21)Application number : 11-015409

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>

(22)Date of filing : 25.01.1999

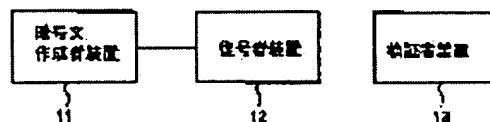
(72)Inventor : ABE MASAYUKI

(54) CIPHER TEXT VERIFYING METHOD, RECORDING MEDIUM AND DEVICE THEREOF

(57)Abstract:

PROBLEM TO BE SOLVED: To verify the propriety of a cipher text without absolutely leaking information about a value in a verification expression by exponentiating a value calculated for verification, when Cramer-Shoup cryptograph is decoded by random numbers whose values are incapable for anyone to know trying to decode it and verifying whether or not the exponentiated result becomes 1.

SOLUTION: Although a cipher text prepared by a cipher text preparing device 11 is decoded by the device 12 of a decoding person, a device 13 of a verifying person verifies whether or not decoding rejection is appropriate so as to avoid rejecting decoding, because it is not a correct cipher text in a self-serving manner. After receiving a cipher text $E=(u1, u2, v, e)$ of a plaintext (m) enciphered by the Cramer-Shoup cryptograph method making X, Y and Z public keys, the device 12 generates a random number (r) and calculates $(c)=H(u1, u2)$ and $(v)=(u1X1+CY1u2X2+CY2V1)r \text{ mod } (p)$. If (v) is 1, this cipher text is deemed accepted, but if (v) is not 1, it is deemed rejected, and the rejection is verified to a third person.



LEGAL STATUS

[Date of request for examination] 26.12.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3302335

[Date of registration] 26.04.2002

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

NOTICES *

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.

2. **** shows the word which can not be translated.

3. In the drawings, any words are not translated.

CLAIMS

Claim(s)]

Claim 1] The cipher verification approach characterized by verifying a cipher by checking whether the value which generated the random number r and squared the value V of an original verification type r in the cipher verification approach verified by checking that the received cipher is made justly and that the value of a verification type is set to 1 is set to 1.

Claim 2] Considering as the big prime factor which divides a clear-cut solution for p to the big prime factor, and divides $p-1$ for q , G_q is multiplicative-group Z_p^* . The subgroup of order q shall be expressed. g_1 and g_2 A logarithm considers as the origin of strange G_q and H is made into a general-purpose Hash Function. dispersion of g_2 which uses g_1 as a bottom -- $(x_1, x_2, y_1, y_2, z) \cdot Z_q^5$ A private key, $1x1g2x2 \bmod p$ of $X=g, 1y1g2of Y=g y2 \bmod p$, and $Z=g1z \bmod p$ (X, Y, Z) are used as a public key. In the code approach to include the cipher E over Plaintext m -- c -- as $H(u_1, u_2) \bmod q$ -- $u_1=g1r \bmod p$ and $u_2=g2r \bmod p$ -- $v=Xr Yc \bmod p$ -- three -- constructing (u_1, u_2, v) -- Decode person equipment is the cipher verification approach characterized by verifying the justification of a cipher by generating a random number r , calculating $c=H(u_1, u_2) \bmod q$, calculating $V=(u_1x_1+cy1u_2 x_2+cy2v-1) r \bmod p$, and checking that V is equal to 1.

Claim 3] The cipher verification approach characterized by proving that it is the result of V calculating like $r \bmod p (u_1x_1+cy1u_2 x_2+cy2v-1)$ in the cipher verification approach of claim 2 to the random number r which uses zero information certification when not equal to 1, and has V to a third party.

Claim 4] Shall consider as the big prime factor which divides a clear-cut solution for p to the big prime factor, and divides $p-1$ for q , and G_q shall express the subgroup of the order q of a multiplicative group Z_p . Make g_1 and g_2 into the origin of G_q , make H into a general-purpose Hash Function, and n persons' decode person is set to P_1-P_n . Each decode person P_j has the open value w_j of a proper, and is $((x_1, x_2, y_1, y_2, z) \cdot Z_q^5$. Distribute with the secrecy variational method of threshold t which fills $3 \leq t \leq n$, and are obtained. The secrecy value $(x_2 j$ and $y_1 j, y_2 x_1 j, j, z_j)$ corresponding to a value w_j is used as the decode person's P_j private key. $X_j=g1x1j g2 x2j \bmod p$, $Y_j=g1y1j g2y2j \bmod p$, and $Z_j=g1zj \bmod p$ (X_j, Y_j, Z_j) are used as the decode person's P_j public key. A safe channel shall be between each decode person equipment. Moreover, each decode person equipment Receiving a content with other all the members' same decode person equipment shall use the broadcast mold channel guaranteed. The decode person P_j shall hold the secrecy value r_j corresponding to a value w_j which distributes random-number $r \cdot Z_q$ with the secrecy variational method of threshold t , and is acquired. $E=(u_1, u_2, v, e)$ is made into the cipher of the plaintext m which used $1x1g2x2 \bmod p$ of $X=g, 1y1g2of Y=g y2 \bmod p$, and $Z=g1z \bmod p$ as the public key. When a right cipher satisfies $u_1=g1r \bmod p$, $u_2=g2r \bmod p$, $c=H(u_1, u_2)$, $v=Xr Yc \bmod p$, and $e=mZr \bmod p$, The equipment of each decode person P_j who received E calculates $c=H(u_1, u_2)$. $V_j=(u_1x_1j+cy1u_2 x2j+cy2v-1) r_j \bmod p$ is calculated. Distribute V_j with a verifiable secrecy variational method $2t$ or less more than threshold t , and are obtained. The equipment of the decode person P_k who transmitted the secrecy value V_{jk} corresponding to a value w_k through the channel safe for each decode person's P_k equipment, and received V_{jk} from all other decode person equipments V_{kj} to which the equipment of each decode person P_j who transmitted V_k to all other decode person equipments, and received V_k corresponds according to a broadcast mold channel is transmitted to all other decode person equipments according to a broadcast mold channel. Each decode person equipment is verified using all $V_{kj}(s)$ to which each V_k received that it was a right value. Choose $2t+1$ piece among the right and checked V_k , and it investigates whether the value V restored with the secrecy restoration procedure to exponent part is equal to 1. If equal and a restoration value is [a secrecy restoration procedure is similarly repeated in other $2t+1$ piece combination and] all equal to 1 about no combination The cipher verification approach characterized by judging that the cipher is inaccurate, and judging the cipher to be the right if there is combination set to 1 at least one.

Claim 5] In the cipher verification approach of claim 4, if the above-mentioned cipher is judged to be the right, w will be used as the n -th root of 1 in $\bmod q$. Each decode person equipment Set w_j to $w_j-1 \bmod q$ and it considers as the characteristic value of disclosure of w_j which fills $w_j! \equiv 1$ in $1 \leq j \leq n$. the dispersion which each decode person's P_j equipment calculates $D_j=u1zj \bmod p$, transmits it to all other decode person equipments according to a broadcast mold channel, and uses as a bottom u_1 which received (D_1, \dots, D_n) -- the cipher verification approach characterized by checking that a logarithm is the codeword of a BCH code.

Claim 6] Considering as the big prime factor which divides a clear-cut solution for p to the big prime factor, and divides $p-1$ for q , G_q is multiplicative-group Z_p^* . The subgroup of order q shall be expressed. g_1 and g_2 A logarithm considers as the origin of strange G_q and H is made into a general-purpose Hash Function. dispersion of g_2 which uses g_1 as a bottom -- $(x_1, x_2, y_1, y_2, z) \cdot Z_q^5$ A private key, $1x1g2x2 \bmod p$ of $X=g, 1y1g2of Y=g y2 \bmod p$, and $Z=g1z \bmod p$ (X, Y, Z) are used as a public key. In the code approach to include the cipher E over Plaintext m -- c -- as $H(u_1, u_2) \bmod q$ -- $u_1=g1r \bmod p$ and $u_2=g2r \bmod p$ -- $v=Xr Yc \bmod p$ -- three -- constructing (u_1, u_2, v) -- Decode person equipment generates a random number r , and calculates $x_1'=x_1$ and $r \bmod q$, $x_2'=x_2$ and $r \bmod q$, $y_1'=y_1$ and $r \bmod q$, and $y_2'=y_2$ and $r \bmod q$. The cipher verification approach characterized by verifying the justification of a cipher by calculating $c=H(u_1, u_2) \bmod q$, calculating $V=u1x1'+cy1'u2 x2'+cy2'v-r \bmod p$, and checking that V is equal to 1 from the received cipher.

Claim 7] In the cipher verification approach of claim 6 when not equal to 1, V decode person equipment (X, Y, V) It receives that it is (x_1, x_2, y_1, y_2, r) . $1x1g2x2 \bmod p$ of $X=g, 1y1g2of Y=g y2 \bmod p$, and $V=u1x1r+cy1r u2x2r+cy2r$ satisfying $v-r \bmod p$ -- zero information certification -- using (x_1, x_2, y_1, y_2) , considering as secrecy The cipher verification approach characterized by what is proved to a verification person.

Claim 8] It is under G_q whose logarithm is strange. dispersion of h to which g and h use g as a bottom in the cipher verification approach of

Claim 7 -- decode person equipment Random numbers r , a_1 , a_2 , b_1 , and b_2 are generated. $R = gr \text{ ha mod } p$, $RX1 = Rx1 \text{ ha1 mod } p$, $RX2 = Rx2 \text{ ha2 mod } p$, R , $RX1$, $RX2$, $RY1$, and $RY2$ are exhibited. $RY1 = Ry1 \text{ hb1 mod } p$ and $RY2 = Ry2 \text{ hb2 mod } p$ -- (X , Y , V , R , $RX1$, $RX2$, $RY1$, $RY2$) receive that it is (x_1 , x_2 , y_1 , y_2 , r , a_1 , a_2 , b_1 , b_2). $1x1g \ 2 \ x2 \text{ mod } p$ of $X=g$, $1y1g \ 2 \ of \ Y=g \ y2 \text{ mod } p$, $V=u1x1r+cy1r \ u2x2r+cy2r \ v \text{ mod } p$, $R=gr \text{ ha mod } p$, $RX1=Rx1 \text{ ha1 mod } p$, $RX2=Rx2 \text{ ha2 mod } p$, $RY1=Ry1 \text{ hb1 mod } p$, and $RY2=Ry2 \text{ hb2 mod } p$ -- the cipher verification approach characterized by proving filling relational expression by zero information certification.

Claim 9] n persons' decode person is set to $P1$ - Pn in the cipher verification approach of claim 6. Use w as the n -th root of 1 in mod q , and w_j is set to $w^{j-1} \text{ mod } q$. $w_j \neq 1$ shall be filled in $1 < j < n$ and a value w_j is assigned to each decode person P_j . The decode person's P_j private key (x_2 and y_1 , j , z_j) Distribute x_1 , x_2 , and (y_1 , y_2 , z) with the secrecy variational method of threshold t which fills $3 < t < n$, and are obtained. Consider as the secrecy value corresponding to a value w_j , and $X_j = g^{1x1j} g^{2x2j} \text{ mod } p$, $Y_j = g^{1y1j} g^{2y2j} \text{ mod } p$, and $Z_j = g^{1zj} \text{ mod } p$ (X_j , Y_j , Z_j) are used as the decode person's P_j public key. A safe channel shall be between each decode person equipment. Moreover, each decode person equipment Receiving a content with other all the members' same decode person equipment shall use the broadcast mold channel guaranteed. The decode person P_j shall hold the secrecy value r_j corresponding to a value w_j which distributes random-number $r^{**}Z_q$ with the secrecy variational method of threshold t , and is acquired. Each decode person's P_j equipment Distribute $r-x_1$, r and x_2 , $r-y_1$, and $r-y_2$ with the secrecy variational method of threshold t , respectively, and are obtained. The equipment of each decode person P_j who calculated and held secrecy value $x1j'$ corresponding to a value w_j , $x2j'$, $y1j'$, and $y2j'$ by the distributed multiplication method, and received the cipher $c=H(u_1, u_2)$ is calculated and $V_j = u1x1j' + cy1j'u2x2j' + cy2j'v-rj \text{ mod } p$ is calculated. According to a broadcast mold channel Transmit V_j to all other decode person equipments, and it checks that the exponent part of ($V1$, --, Vn) is the codeword of a BCH code. The cipher verification approach characterized by verifying the justification of a cipher by checking that the value V restored with the secrecy restoration procedure to exponent part is equal to 1.

Claim 10] In the cipher verification approach of claim 9, $2t < n$ shall be filled for threshold t . Instead of checking that the exponent part of ($V1$, --, Vn) is the codeword of a BCH code Each decode person's P_j equipment without leaking the information concerning [that V_j is as a result of / of $u1x1j' + cy1j'u2x2j' + cy2j'v-rj \text{ mod } p$ / right count, and] $x1j'$, $x2j'$, $y1j'$, $y2j'$, and r_j The cipher verification approach characterized by proving to other decode person equipments, specifying the decode person P_j in whom zero information certification failed as a deviation person, and other decode person equipments restoring a deviation person's secrecy value $x1j'$, $x2j'$, $y1j'$, $y2j'$, and r_j using secrecy value recovery procedure by zero information certification.

Claim 11] When ($V1$, --, Vn) are not the codewords of a BCH code, in the cipher verification approach of claim 9 each decode person's P_j equipment Without leaking the information concerning [that V_j is as a result of / of $u1x1j' + cy1j'u2x2j' + cy2j'v-rj \text{ mod } p$ / count, and] $x1j'$, $x2j'$, $y1j'$, $y2j'$, and r_j Prove to other decode person equipments by zero information certification, and the equipment of the decode person P_j who failed in certification is specified with a deviation person's equipment. The cipher verification approach characterized by other decode person equipments restoring secrecy value $x1j'$ of a deviation person's equipment, $x2j'$, $y1j'$, $y2j'$, and r_j using secrecy value recovery procedure.

Claim 12] the dispersion each decode person's P_j equipment calculates $D_j = u1zj \text{ mod } p$, and whose value V which carried out [above-mentioned] restoration transmits to all other decode person equipments according to a broadcast mold channel, and uses as a bottom $u1$ which received ($D1$, --, Dn) in the cipher verification approach of claim 9 when equal to 1 -- the cipher verification approach characterized by to check that a logarithm is the codeword of a BCH code.

Claim 13] The restored value V in the cipher verification approach of claim 10 when equal to 1 Without each decode person's P_j equipment calculating $D_j = u1zj \text{ mod } p$, and leaking the information concerning [that D_j is as a result of right count, and] z_j The cipher verification approach characterized by proving to other decode persons, specifying the decode person P_j who failed in zero information certification as a deviation person, and other decode person equipments restoring a deviation person's secrecy value z_j using secrecy value recovery procedure by zero information certification.

Claim 14] It is the cipher verification approach characterized by for the secrecy restoration procedure to the exponent part to which each decode person equipment uses $u1$ as a bottom from the right ($D1$, --, Dn) in claim 12 or the cipher verification approach of 13 restoring $D = u1z \text{ mod } p$, calculating $m = e/D \text{ mod } p$, and decoding Plaintext m .

Claim 15] Shall consider as the big prime factor which divides a clear-cut solution for p to the big prime factor, and divides $p-1$ for q , and Gq shall express the subgroup of the order p of a multiplicative group Zp . Make $g1$ and $g2$ into the origin of Gp , make H into a general-purpose Hash Function, and it considers as the public key which uses $1x1g \ 2 \ x2 \text{ mod } p$ of $X=g$, $1y1g \ 2 \ of \ Y=g \ y2 \text{ mod } p$, and $Z=g^{1z} \text{ mod } p$ for an encryption procedure. (x_1 , x_2 , y_1 , y_2 , z) $**Z_q$ It contains. $**$ -- the cipher [as opposed to / carry out and / Plaintext m] E -- c -- as $H(u_1, u_2) \text{ mod } p$ -- $u1=g1r \text{ mod } p$ and $u2=g2r \text{ mod } p$ -- $v=Xr \ Yc \text{ mod } p$ -- three -- constructing (u_1 , u_2 , v) -- The processing which generates a random number r , the processing which receives Cipher E , and the processing which calculates $c=H(u_1, u_2) \text{ mod } q$. The record medium which recorded the program which makes the computer of decode person equipment perform processing which calculates $V=(u1x1+cy1u2x2+cy2v-1)r \text{ mod } p$, and processing which checks that it is $V=1$ and verifies the justification of a cipher.

Claim 16] $V1=1$ The processing which will exhibit BC (r) using a bit commitment function (BC) if it becomes, r which constitutes BC (r), x_1 which constitutes public keys X and Y , x_2 , and y_1 and y_2 are used. ($u1x1+cy1u2x2+cy2v-1$) The record medium characterized by including the program which performs processing proved to a third party by zero information certification, without leaking the secrecy concerning [that the result of having performed count which becomes $r \text{ mod } p$ is V , and] r , x_1 , x_2 , and y_1 and y_2 .

Claim 17] Shall consider as the big prime factor which divides a clear-cut solution for p to the big prime factor, and divides $p-1$ for q , and Gq shall express the subgroup of the order q of a multiplicative group Zp . Make $g1$ and $g2$ into the origin of Gq , make H into a general-purpose Hash Function, and n persons' decode person is set to $P1$ - Pn . each decode person P_j -- the open value w_j of a proper -- having -- $** (x_1, x_2, y_1, y_2, z)$ Z_q Distribute with the secrecy variational method of threshold t which fills $3 < t < n$, and are obtained. The secrecy value (x_2 and y_1 , j , z_j) corresponding to a value w_j is used as the decode person's P_j private key. $X_j = g^{1x1j} g^{2x2j} \text{ mod } p$, $Y_j = g^{1y1j} g^{2y2j} \text{ mod } p$, and $Z_j = g^{1zj} \text{ mod } p$ are used as the decode person's P_j public key. The processing which generates the secrecy value r_j corresponding to the value w_j which distributes random-number $r^{**}Z_q$ with the secrecy variational method of threshold t , and is acquired, $1x1g \ 2 \ x2 \text{ mod } p$ of $X=g$, $1y1g \ 2 \ of \ Y=g \ y2 \text{ mod } p$, and $Z=g^{1z} \text{ mod } p$ are used as a public key. It considers as the cipher of Plaintext m . A right cipher $u1=g1r \text{ mod } p$, $u2=g2r \text{ mod } p$, $c=H(u_1, u_2)$, The processing which fills $v=Xr \ Yc \text{ mod } p$ and $e=mZr \text{ mod } p$, and receives cipher $E=(u_1, u_2, v, e)$, The processing which calculates $c=H(u_1, u_2)$, and the processing which calculates $V_j=(u1x1j+cy1ju2x2j+cy2jv-1)rj \text{ mod } p$, The processing which transmits the secrecy value V_jk corresponding to a value w_k which distributes V_j with a verifiable secrecy variational method $2t$ or less more than threshold

, and is acquired to each decode person's Pk equipment, The processing which receives Vkj from all other decode person equipments Pk, and he processing which transmits Vj to all other decode person equipments, The processing which receives Vk from all other decode person equipments, and the processing which transmits Vkj to all other decode person equipments, every -- with the processing which verifies that Vk is a right value using Vkj from all other decode person equipments Choose 2t+1 piece among the right and checked Vk, and it investigates whether the value V restored with the secrecy restoration procedure to exponent part is equal to 1. If equal and a restoration value is [a secrecy restoration procedure is similarly repeated in other 2t+1 piece combination and] all equal to 1 about no combination The record medium which recorded the program which makes the computer of decode person equipment perform processing which judges that the cipher is inaccurate, and will judge the cipher to be the right if there is combination set to 1 at least one.

[Claim 18] Shall consider as the big prime factor which divides a clear-cut solution for p to the big prime factor, and divides p-1 for q, and Gq shall express the subgroup of the order q of a multiplicative group Zp. g1 and g2 are made into the origin of Gq, H is made into a general-purpose Hash Function, and it is $^{**}(x1, x2, y1, y2, z) Zq5$. Private key, $1x1g2x2mod p$ of $X=g$, $1y1g2of Y=g y2mod p$, and $Z=g1z mod p$ (X, Y, Z) are used as a public key. the cipher E over Plaintext m -- c -- as $H(u1, u2) mod q$ -- $u1=g1r mod p$ and $u2=g2r mod p$ -- $v=Xr Ycmod p$ -- three -- constructing (u1, u2, v) -- it containing and with the processing which generates a random number r The processing which calculates $x1'=x1$ and $rmod q$, $x2'=x2$ and $rmod q$, $y1'=y1$ and $rmod q$, and $y2'=y2$ and $rmod q$ using Above r, The processing which receives Cipher E, and the processing which calculates $c=H(u1, u2) mod q$, and calculates $V=u1x1'+cy1' u2 x2'+cy2' v-rmod p$ from the received cipher, The record medium which recorded the program which makes the computer of decode person equipment perform processing which verifies the justification of a cipher when Above V checks that it is equal to 1.

[Claim 19] In the record medium of claim 18 when not equal to 1, V (X, Y, V) It receives that it is (x1, x2, y1, y2, r). $1x1g2x2mod p$ of $X=g$, $1y1g2of Y=g y2mod p$, and $V=u1x1r+cy1r$ satisfying $u2 x2r+cy2r v-rmod p$ -- zero information certification -- using (x1, x2, y1, y2, r), considering as secrecy The record medium characterized by the above-mentioned program including the program which makes the above-mentioned computer perform processing proved to a verification person.

[Claim 20] dispersion of h to which g and h use g as a bottom in the record medium of claim 19 -- with the processing which is under Gq whose logarithm is strange and generates random numbers r, a1, a2, b1, and b2 $R=gr ha mod p$, $RX1=Rx1ha1mod p$, $RX2=Rx2ha2mod p$, $RY1=Ry1hb1mod p$ and $RY2=Ry2hb2mod p$ -- with the processing which exhibits R, RX1, RX2, RY1, and RY2 (X, Y, V, R, RX1, RX2, RY1, RY2) receive that it is (x1, x2, y1, y2, r, a, a1, a2, b1, b2). $1x1g2x2mod p$ of $X=g$, $1y1g2of Y=g y2mod p$, $V=u1x1r+cy1r$ $u2x2r+cy2r v-rmod p$, $R=gr ha mod p$, $RX1=Rx1ha1mod p$, $RX2=Rx2ha2mod p$, $RY1=Ry1hb1mod p$, and $RY2=Ry2hb2mod p$ -- the record medium characterized by the above-mentioned program including the program which makes the above-mentioned computer perform processing which proves filling relational expression by zero information certification.

[Claim 21] In the record medium of claim 18, set n persons' decode person to P1-Pn, and w is used as the n-th root of 1 in mod q. Shall set wj to $wj-1 mod q$ and $wj!=1$ shall be filled in $1<j<n$. A value wj is assigned to each decode person Pj. The decode person's Pj private key (x2j and y1j, y2x1j, j, zj) Distribute x1, x2, and (y1, y2, z) with the secrecy variational method of threshold t which fills $3<t<n$, and are obtained. Consider as the secrecy value corresponding to a value wj, and $Xj=g1x1j g2x2j mod p$, $Yj=g1y1j g2y2j mod p$, and $Zj=g1zjmod p$ (Xj, Yj, Zj) are used as the decode person's Pj public key. Processing holding the secrecy value rj corresponding to a value wj which distributes random-number $r^{**}Zq$ with the secrecy variational method of threshold t, and is acquired, The processing which calculates and holds secrecy value x1j' corresponding to a value wj which distributes rx1, rx2, ry1, and ry2 with the secrecy variational method of threshold t, respectively, and is obtained, x2j', y1j', and y2j' by the distributed multiplication method, If a cipher is received, $c=H(u1, u2)$ will be calculated and $Vj=u1x1j'+cy1j'u2x2j'+cy2j'v-rj mod p$ will be calculated. According to a broadcast mold channel The processing which transmits Vj to all other decode person equipments, and the processing which checks that the exponent part of (V1, --, Vn) is the codeword of a BCH code, The record medium characterized by the above-mentioned program including the program which performs processing which verifies the justification of a cipher by checking that the value V restored with the secrecy restoration procedure to the above-mentioned exponent part is equal to 1 by above-mentioned computer.

[Claim 22] In the record medium of claim 21, $2<t<n$ shall be filled for threshold t. Instead of the processing which checks that the exponent part of (V1, --, Vn) is the codeword of a BCH code Without leaking the information concerning [that Vj is as a result of / of $u1x1j'+cy1j'u2x2j'+cy2j'v-rj mod p$ / right count, and] x1j', x2j', y1j', y2j', and rj The processing proved to other decode persons by zero information certification and the decode person Pj in whom zero information certification failed are specified as a deviation person. The record medium characterized by including the program which makes the above-mentioned computer perform a deviation person's secrecy value x1j', x2j', y1j', y2j', and processing that restores rj using secrecy value recovery procedure in the above-mentioned program.

[Claim 23] In the record medium of claim 21, when (V1, --, Vn) are not the codewords of a BCH code Without leaking the information concerning [that Vj is as a result of / of $u1x1j'+cy1j'u2x2j'+cy2j'v-rj mod p$ / count, and] x1j', x2j', y1j', y2j', and rj The processing proved to other decode persons by zero information certification and the decode person Pj who failed in the above-mentioned certification are specified with a deviation person. The record medium characterized by the above-mentioned program including the program which makes the above-mentioned computer perform processing which restores a deviation person's secrecy value x1j', x2j', y1j', y2j', and rj using secrecy value recovery procedure.

[Claim 24] Shall consider as the big prime factor which divides a clear-cut solution for p to the big prime factor, and divides p-1 for q, and Gq shall express the subgroup of the order q of a multiplicative group Zp. g1 and g2 are made into the origin of Gq, H is made into a general-purpose Hash Function, and it is $^{**}(x1, x2, y1, y2, z) Zq5$. Private key, $1x1g2x2mod p$ of $X=g$, $1y1g2of Y=g y2mod p$, and $Z=g1z mod p$ (X, Y, Z) are used as a public key. It is verification equipment of the cipher to include. the cipher E over Plaintext m -- c -- as $H(u1, u2) mod q$ -- $u1=g1r mod p$ and $u2=g2r mod p$ -- $v=Xr Ycmod p$ -- three -- constructing (u1, u2, v) -- A means to generate a random number r, and a means to calculate $c=H(u1, u2) mod q$, Cipher verification equipment characterized by having a means to calculate $V=(u1x1+cy1u2 x2+cy2v-1) r mod p$, and a means to verify the justification of a cipher when V checks that it is equal to 1.

[Claim 25] Cipher verification equipment characterized by having a means to prove that it is the result of V's using zero information certification when not equal to 1, and V calculating like $r mod p (u1x1+cy1u2 x2+cy2v-1)$ to a random number r in the cipher verification equipment of claim 24 for a third party.

[Claim 26] Shall consider as the big prime factor which divides a clear-cut solution for p to the big prime factor, and divides p-1 for q, and Gq shall express the subgroup of the order q of a multiplicative group Zp. Make g1 and g2 into the origin of Gq, make H into a general-purpose

Hash Function, and n persons' decode person is set to P_1 - P_n . each decode person P_j -- the open value w_j of a proper -- having -- $*(x_1, x_2, y_1, z)$ Zq_5 Distribute with the secrecy variational method of threshold t which fills $3 \leq t \leq n$, and are obtained. The secrecy value $(x_2$ and y_1 j, y_2 $\leq j, j, z_j)$ corresponding to a value w_j is used as the decode person's P_j private key. $X_j = g^{x_1} g^{x_2} \bmod p$, $Y_j = g^{y_1} g^{y_2} \bmod p$, and $Z_j = g^{z_j} \bmod p$ (X_j, Y_j, Z_j) are used as the decode person's P_j public key. A safe channel shall be between each decode person equipment. Moreover, each decode person equipment Receiving a content with other all the members' same decode person equipment shall use the broadcast mold channel guaranteed. The decode person P_j shall hold the secrecy value r_j corresponding to a value w_j which distributes random-number $r^{**}Zq$ with the secrecy variational method of threshold t , and is acquired. $E = (u_1, u_2, v, e)$ is made into the cipher over the plaintext m which used $1 \times g^2 \times 2 \bmod p$ of $X = g$, $1 \times g^2$ of $Y = g^2 \bmod p$, and $Z = g^{z_j} \bmod p$ as the public key. A right cipher $u_1 = g^{r_j} \bmod p$, $u_2 = g^{2r_j} \bmod p$, $v = H(u_1, u_2)$, A means to be verification equipment of the cipher with which are satisfied of $v = X^r Y^r \bmod p$ and $e = m Z^r \bmod p$, and to calculate $c = H(u_1, u_2)$ by receiving E , A means to calculate $V_j = (u_1^{x_1} j + c y_1 u_2^{x_2} j + c y_2 j - 1) r_j \bmod p$, V_j is distributed with a verifiable secrecy variational method $2t$ or less more than threshold t . When V_{kj} is received from a means to acquire the secrecy value V_{jk} corresponding to a value w_k , a means to transmit V_{jk} through a channel safe for each decode person's P_k equipment, and all other decode person equipments P_k , according to a broadcast mold channel If a means to transmit V_j to all other decode person equipments, and V_k are received A means to transmit corresponding V_{kj} to all other decode person equipments according to a broadcast mold channel, every -- with a means to verify using V_{kj} that V_k is a right value, and a means to choose $2t+1$ piece among the right and checked V_k , and to restore V with the secrecy restoration procedure to exponent part A means to investigate whether the restored value V is equal to 1, and a means by which will repeat a secrecy restoration procedure similarly in other $2t+1$ piece combination if it becomes, and V investigates [which is not equal to 1] whether V is equal to 1, Cipher verification equipment characterized by having a means to judge that the cipher is inaccurate if a restoration value is all equal to 1 about no $2t+1$ piece combination, and to judge the cipher to be the right if there is combination set to 1 at least one.

[Claim 27] w is used as the n -th root of 1 in mod q in the cipher verification equipment of claim 26. Each decode person A means to set w_j to $w_j - 1 \bmod q$, to consider as the characteristic value of disclosure of w_j which fills $w_j! = 1$ in $1 \leq j \leq n$, and to calculate $D_j = u_1^{z_j} \bmod p$, a means to transmit D_j to all other decode person equipments according to a broadcast mold channel, and the dispersion which uses as a bottom u_1 which received (D_1, \dots, D_n) -- the cipher verification equipment characterized by having a means to check that a logarithm is the codeword of a BCH code.

[Claim 28] Shall consider as the big prime factor which divides a clear-cut solution for p to the big prime factor, and divides $p-1$ for q , and G_q shall express the subgroup of the order q of a multiplicative group Z_p . g_1 and g_2 are made into the origin of G_q , H is made into a general-purpose Hash Function, and it is $*(x_1, x_2, y_1, y_2, z)$ Zq_5 . Private key, $1 \times g^2 \times 2 \bmod p$ of $X = g$, $1 \times g^2$ of $Y = g^2 \bmod p$, and $Z = g^{z_j} \bmod p$ (X, Y, Z) are used as a public key. It is verification equipment of the cipher to include. the cipher E over Plaintext m -- c -- as $H(u_1, u_2) \bmod q$ -- $u_1 = g^{r_j} \bmod p$ and $u_2 = g^{2r_j} \bmod p$ -- $v = X^r Y^r \bmod p$ -- three -- constructing (u_1, u_2, v) -- A means to generate a random number r , and a means to calculate $x_1' = x_1$ and $r \bmod q$, $x_2' = x_2$ and $r \bmod q$, $y_1' = y_1$ and $r \bmod q$, and $y_2' = y_2$ and $r \bmod q$, A means to calculate $c = H(u_1, u_2) \bmod q$ from the received cipher, Cipher verification equipment characterized by having a means to calculate $V = u_1^{x_1'} + c y_1' u_2^{x_2'} + c y_2' v - r \bmod p$, and a means to verify the justification of a cipher when V checks that it is equal to 1 from this count result and a receiving cipher.

[Claim 29] In the cipher verification equipment of claim 28 V when not equal to 1 (X, Y, V) It receives that it is (x_1, x_2, y_1, y_2, r) . $1 \times g^2 \times 2 \bmod p$ of $X = g$, $1 \times g^2$ of $Y = g^2 \bmod p$, and $V = u_1^{x_1} + c y_1 u_2^{x_2} + c y_2 r$ satisfying $v - r \bmod p$ -- zero information certification -- using (x_1, x_2, y_1, y_2, r) , considering as secrecy Cipher verification equipment characterized by having a means to prove to verification person equipment.

[Claim 30] dispersion of h to which g and h use g as a bottom in the cipher verification equipment of claim 29 -- with a means to be under G_q whose logarithm is strange and to generate random numbers r, a_1, a_2, b_1 , and b_2 $R = g^r h^a \bmod p$, $RX_1 = R^{x_1} h^{a_1} \bmod p$, $RX_2 = R^{x_2} h^{a_2} \bmod p$, $RY_1 = R^{y_1} h^{b_1} \bmod p$ and $RY_2 = R^{y_2} h^{b_2} \bmod p$ -- with a means to exhibit R, RX_1, RX_2, RY_1 , and RY_2 ($X, Y, V, R, RX_1, RX_2, RY_1, RY_2$) receive that it is $(x_1, x_2, y_1, y_2, r, a, a_1, a_2, b_1, b_2)$. $1 \times g^2 \times 2 \bmod p$ of $X = g$, $1 \times g^2$ of $Y = g^2 \bmod p$, $V = u_1^{x_1} + c y_1 u_2^{x_2} + c y_2 r - v - r \bmod p$, $R = g^r h^a \bmod p$, $RX_1 = R^{x_1} h^{a_1} \bmod p$, $RX_2 = R^{x_2} h^{a_2} \bmod p$, $RY_1 = R^{y_1} h^{b_1} \bmod p$, and $RY_2 = R^{y_2} h^{b_2} \bmod p$ -- the cipher verification equipment characterized by having a means to prove filling relational expression by zero information certification.

[Claim 31] n persons' decode person is set to P_1 - P_n in the cipher verification equipment of claim 28. Use w as the n -th root of 1 in mod q , and w_j is set to $w_j - 1 \bmod q$. In $1 \leq j \leq n$, shall fill $w_j! = 1$ and a value w_j is assigned to each decode person P_j . (x_1, x_2, y_1, y_2, z) $^{**}Zq_5$ Consider as a private key and $1 \times g^2 \times 2 \bmod p$ of $X = g$, $1 \times g^2$ of $Y = g^2 \bmod p$, and $Z = g^{z_j} \bmod p$ are used as a public key. The decode person's P_j private key $(x_2$ and y_1 j, y_2 $\leq j, j, z_j)$ Distribute x_1, x_2 , and (y_1, y_2, z) with the secrecy variational method of threshold t which fills $3 \leq t \leq n$, and are obtained. Consider as the secrecy value corresponding to a value w_j , and $X_j = g^{x_1} g^{x_2} \bmod p$, $Y_j = g^{y_1} g^{y_2} \bmod p$, and $Z_j = g^{z_j} \bmod p$ (X_j, Y_j, Z_j) are used as the decode person's P_j public key. A safe channel shall be between each decode person equipment. Moreover, each decode person equipment Receiving a content with other all the members' same decode person equipment shall use the broadcast mold channel guaranteed, and it distributes random-number $r^{**}Zq$ with the secrecy variational method of threshold t . rx_1, rx_2, ry_1 , and ry_2 are distributed with the secrecy variational method of threshold t with a means to acquire the secrecy value r_j corresponding to a value w_j , respectively. A means to calculate and obtain secrecy value $x_1'j$ corresponding to a value w_j , $x_2'j$, $y_1'j$, and $y_2'j$ by the distributed multiplication method, About the received cipher, according to a means to calculate $c = H(u_1, u_2)$, a means to calculate $V_j = u_1^{x_1'j} + c y_1'j u_2^{x_2'j} + c y_2'j v - r_j \bmod p$, and a broadcast mold channel A means to transmit V_j to all other decode person equipments, and a means to check that the exponent part of (V_1, \dots, V_n) is the codeword of a BCH code, Cipher verification equipment characterized by having a means to restore V with the secrecy restoration procedure to exponent part, and a means to verify the justification of a cipher by checking that the restored value V is equal to 1.

[Claim 32] In the cipher verification equipment of claim 31, $2 \leq t \leq n$ shall be filled for threshold t . Instead of checking that the exponent part of (V_1, \dots, V_n) is the codeword of a BCH code Without leaking the information concerning [that V_j is as a result of / of $u_1^{x_1'j} + c y_1'j u_2^{x_2'j} + c y_2'j v - r_j \bmod p$ / right count, and] $x_1'j, x_2'j, y_1'j, y_2'j$, and r_j Cipher verification equipment characterized by having a means to prove to other decode persons by zero information certification.

[Claim 33] In the cipher verification equipment of claim 31, when (V_1, \dots, V_n) are not the codewords of a BCH code Without leaking the information concerning [that V_j is as a result of / of $u_1^{x_1'j} + c y_1'j u_2^{x_2'j} + c y_2'j v - r_j \bmod p$ / count, and] $x_1'j, x_2'j, y_1'j, y_2'j$, and r_j Cipher verification equipment which specifies a means to prove to other decode persons by zero information certification, and the decode person P_j who failed in the certification with a deviation person, and is characterized by having a deviation person's secrecy value $x_1'j, x_2'j, y_1'j, y_2'j$, and a means to restore r_j using secrecy value recovery procedure.

Translation done.]

THIS PAGE BLANK (USPTO)

NOTICES *

IPPO and NCIPI are not responsible for any damages caused by the use of this translation.

This document has been translated by computer. So the translation may not reflect the original precisely.

**** shows the word which can not be translated.

In the drawings, any words are not translated.

DETAILED DESCRIPTION

Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the cipher verification approach that a decode person verifies the justification of a cipher especially, and its program documentation medium, about the safe code approach that the information about a decode person's private key does not leak, also when the content of a communication link is kept secret when communicating by the electrical-communication system, and the content of decode is exhibited.

[0002]

[Description of the Prior Art] In a cryptosystem strong against a selection plaintext attack, a decode person verifies that the transmitting person of a cipher knows the original plaintext by a certain approach. A Cramer-Shoup code Paper R.Cramer and V.Shoup: "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack", Advances in Cryptology-CRYPTO'98 and LNCS 1462, Springer-Verlag, pp.13-25, and 1998. It is the public-key-encryption approach that it can prove that it is strong to an accommodative selection cipher attack under an assumption which is called existence of a general purpose one direction nature Hash Function and the difficulty of a Diffie-Hellman judging problem and which is believed widely. A Cramer-Shoup code is the code approach supposing one person's decode person with one private key corresponding to one public key.

[0003] By the Cramer-Shoup code approach that it is already known in the case of the 1 decode person that it is strong to an accommodative selection cipher attack First, choose the big prime factors p and q so that q may divide $p-1$, and the origin g_1 and g_2 of the subgroup G_q of the order q of a multiplicative group Z_p is used. It is $((x_1, x_2, y_1, y_2, z) \in Z_q^5$ about a private key. A public key is set to $1x_1g_1 + 2x_2 \bmod p$ of $X=g_1y_1g_2$ of $Y=g_2y_2 \bmod p$, and $Z=g_1z \bmod p$. The cipher E over plaintext $m \in G_q$ consists of (u_1, u_2, v, e) , and the cipher created correctly satisfies $u_1 = g_1r \bmod p$, $u_2 = g_2r \bmod p$, $c = H(u_1, u_2)$, $v = Xr \bmod p$, and $e = mZr \bmod p$ to a certain random number r . First, $c = H(u_1, u_2)$ is calculated and it verifies whether a cipher fills verification type $u_1x_1 + cy_1u_2x_2 + cy_2 \bmod p$, the decode person who received this cipher refuses decode of that cipher, when not filling, when filling, calculates $m = e/u_1z \bmod p$ and gets Plaintext m .

[0004] By the above-mentioned verification type, a decode person can check that the maker of a cipher knows the original plaintext m . Since decode is refused to the unjust cipher with which a verification type is not filled, as for an aggressor, information with useful any is not acquired, either. However, when refusing decode by this cipher verification approach as a result of verification, it is actually difficult to prove the information concerning [that the cipher verified to the third party does not serve as $V = v \bmod p$ as inaccurate / 2 (mod p) / , i.e., $V = u_1x_1 + cy_1u_2x_2 + cy_2$, and] V , without leaking information in any way.

[0005] Furthermore, by secrecy distribution distributing a corresponding private key to two or more partial private keys to one public key, and making this hold to two or more decode persons so that it may often be carried out by an ElGamal cryptosystem etc. As opposed to an unjust cipher with which a verification type is not filled in this code decode approach when the decode person of the manpower exceeding a threshold cooperates and it applies the decode with a threshold which enables it to decode a cipher Since the count result V of left part $u_1x_1 + cy_1u_2x_2 + cy_2$ of a verification type becomes known to two or more decode persons, when the decode person who conspired with the aggressor exists, information is revealed to an aggressor and the safety to a selection cipher attack cannot be maintained.

[0006] the decode approach with a threshold -- paper V.Shoup and R.Gennaro: "Securing threshold cryptosystems against chosen ciphertext attack", Advances in Cryptology-EUROCRYPT, 98, LNCS 1403, Springer-Verlag, and pp.1- 16 and 1998 It is shown under an assumption called existence of random Oracle that the proposed method is strong to an accommodative selection cipher attack.

[0007] However, an assumption called random Oracle can obtain no guarantee about the safety, when it is very unreal and random Oracle is replaced and used for the Hash Function considered that the usual collision is difficult.

[0008]

[Problem(s) to be Solved by the Invention] In a Cramer-Shoup code, the object of this invention, without leaking the information about the value in a verification type entirely When the justification of a cipher can be verified and it is shown that the value of a verification type is not just When the decode person of further plurality [prove / for a third party] cooperates and verifies that the value is created correctly by zero information certification, even if there is an inaccurate person in a decode person The value of a verification type is to offer the cipher verification approach which is not revealed to a decode person, either, its program documentation medium, and its equipment.

[0009]

[Means for Solving the Problem] The exponentiation of the value of the verification type at the time of the decode in a Cramer-Shoup code is carried out with the random number with which everyone of a decode person cannot know the value, and the justification of a cipher is verified by verifying whether the result of having carried out the exponentiation is set to 1. Count of carrying out a exponentiation by these random numbers, by carrying out by cooperation of a total-session person by distributed count Also when not filling a verification type, the value of the verification type before carrying out a exponentiation is revealed to no decode person, and it is got blocked. When not just Since calculated value turns into a value which is not 1 and the exponentiation of the value is carried out by the random numbers, even if the value by which the exponentiation is carried out is shown and it is shown that calculated value is not 1, i.e., are not just, the value in front of the exponentiation is hidden, and there is no possibility that information may leak.

0010] Setting n persons' decode person to $P1-Pn$, each decode person Pj ($j=1, 2, \dots, n$) shall have the open value wj of a proper. ($x1, x2, y1, z$) $**Zq5$ It distributes with the secrecy variational method of threshold t , and let the secrecy value ($x2j$ and $y1j, y2x1j, j, zj$) corresponding to a value wj be the decode person's Pj private key.

0011] Moreover, let $Xj=g^{x1}l^{x2} \bmod p$, $Yj=g^{y1}l^{y2} \bmod p$, and $Zj=g^{z1} \bmod p$ (Xj, Yj, Zj) be the decode person's Pj public keys. It considers as the public key which uses $l^{x1}g^{x2} \bmod p$ of $X=g, l^{y1}g^{y2}$ of $Y=g^{y2} \bmod p$, and $Z=g^{z1} \bmod p$ (X, Y, Z) for encryption. It shall connect by the safe channel between each decode person equipment, and each decode person equipment shall use the broadcast mold channel it is guaranteed to be to receive a content with other all the members' same decode person equipment.

0012] $E=(u1, u2, v, e)$ is made into the cipher of the plaintext m enciphered by the Cramer-Shoup code approach. Decode person equipment performs a distributed random-number generation procedure in cooperation, and the decode person's Pj equipment acquires the secrecy value j . Here, rj is a secrecy value corresponding to the value wj at the time of distributing random-number $r**Zq$ with the secrecy variational method of threshold t , and is the value which can recover r with a secrecy decode procedure from the secrecy value of $t+1$ piece of arbitration. Moreover, each decode person equipment cannot know the value of r , but r becomes the random integer of under or more $0q$ from the property of a distributed random-number generation procedure.

0013] The equipment of each decode person Pj who received E calculates $c=H(u1, u2)$ and $Vj=(u1x1j+cy1ju2x2j+cy2jv-1)rj \bmod p$. Furthermore, Vj is distributed with a with a threshold $[0.2t]$ verifiable secrecy variational method, and the secrecy value Vjk corresponding to a value wk ($k=1, 2, \dots, n, k!=j$) is transmitted through a channel safe for each decode person's Pk equipment. After receiving Vjk from all other decode person equipments, the decode person's Pk equipment transmits Vk to all other decode person equipments through a broadcast mold channel. As for each decode person equipment, each Vk which received verifies using Vkj that it is a right value.

0014] $2t+1$ piece is chosen among the right and checked Vk , and it investigates whether the value V restored with the secrecy restoration procedure to exponent part, i.e., $x1k+cy1k$, and $x2k+cy2k$ is equal to 1. If not equal, a secrecy restoration procedure will be similarly repeated on other combination, and if a restoration value is all equal to 1 about no $2t+1$ piece combination, decode will be refused and it will stop.

0015] the private key restoration procedure as opposed to [when each decode person equipment calculates according to the above-mentioned procedure] the exponent part from the right Vk of the arbitration beyond $2t+1$ piece -- $V=(u1x1+cy1u2x2+cy2v-1)r \bmod p$ -- V can be restored. here, in cooperation with [V/V makes p law and] 1 -- if it becomes -- Cramer-Shoup -- in cooperation with [the original value of verification type $u1x1+cy1u2x2+cy2$ in law] v . On the other hand, when V becomes in cooperation with 1, it is in cooperation with [an original verification type] v or a random number r is 0. However, the probabilities for the random number r generated in the distributed random-number generation procedure to be set to 0 are $1/q$, and since they are small enough, they can be disregarded. Therefore, V can consider in cooperation with [an original verification type] v , when in cooperation with 1.

0016] Here, it is assumed that there are a maximum of t decode persons who commit injustice. these t persons -- (1) -- it is made for the value V of the verification type to the unjust cipher E to be set to 1 -- (2) -- it can deviate from the above-mentioned procedure for two kinds of the object of $**$ of making it the value V of the verification type to the just cipher E not set to 1 [or] First, in order to make the object of (1) successful, it must be made for the value of V restored from a certain $2t+1$ piece Vk to be set to 1. However, before all decode person equipments including inaccurate person equipment get to know the value of Vk which other decode person equipments take out Since the value of Vk of self-equipment cannot be changed after having to distribute the value of one's Vk by the verifiable secrecy distribution approach and getting to know the value of Vk of other decode person equipments Only when the anticipation about Vk of other decode person equipments comes true, an inaccurate decode person can attain the object of (1). The probabilities for anticipation to come true are $1/q$, and since they are small enough, they can be disregarded. Next, since an inaccurate person is at most t persons and, as for other $2t+1$ person equipments, the right value is transmitted even if inaccurate decode person equipment transmits what kind of unjust value Vk about the case of (2), the whole of at least one kind can take the set which consists of $2t+1$ piece Vk of a right value, and $V=1$ is restored from such a set.

0017] Since one value of r which fills $V=(u1x1+cy1u2x2+cy2v-1)r \bmod p$ to any values of $u1x1+cy1u2x2+cy2$ about informational leakage when V is not 1 becomes settled Even if the value of $(u1x1+cy1u2x2+cy2v-1)$ is randomized by r and shows this randomized value, the value before being randomized by r does not leak, that is, the information about $u1x1+cy1u2x2+cy2$ does not leak at all by the above-mentioned verification approach.

0018] As mentioned above, without leaking the information about a private key entirely, if the decode person who commits injustice according to this invention is less than [of all decode persons] $1/3$, by cooperation of two or more decode person, it is possible to calculate a verification type equivalent to the verification type of the original Cramer-Shoup code approach, and, therefore, two or more decode person's code decode equipment strong against an accommodative selection cipher attack can be constituted.

0019] When n decode persons are in the above technique, to n data for verification ($V1, \dots, Vn$) received from all decode person equipments, each decode person equipment takes out $2t+1$ piece data, and verifies whether a certain verification type is satisfied. When not satisfied, this verification is performed to all the $2t+1$ piece combination that can be taken to n pieces. Therefore, in not satisfying a verification type, it has the fault that computational complexity increases exponentially, to several n of a decode person.

0020] According to another viewpoint of this invention, in the code decode approach by two or more decode persons, the cipher verification approach and its program documentation medium of a code strong against the accommodative selection cipher attack which can be recovered even if it can perform count efficiently also to many decode persons and $1/3$ or more decode persons perform injustice are offered. That is, as a means to reduce the computational complexity to the number of decode persons, by making each decode person equipment prove the justification of that result by zero information certification, an inaccurate person is specified and, according to another viewpoint of this invention, a cipher is first verified only using just data. By doing so, it is possible to verify by the computational complexity proportional to several n of a decode person. However, since there is much traffic, when injustice hardly happens, effectiveness is bad [the zero information certification used in this case]. When a right cipher is received by setting the open value of each decode person's proper that the count result of each decode person equipment serves as a codeword of a BCH code, and addressee equipment verifying that a count result is a codeword, and performing zero information certification only when it is not a codeword, it becomes possible to perform efficient count, with traffic stopped.

0021] If based on this approach, the number of the inaccurate persons who can approve is to t persons who fill $3t+1>n$, and when a safe system with more high tolerance is desired, it is unsuitable. Moreover, although it also becomes bored when an inaccurate person is less than [$1/3$ or more] $1/2$, and other decode person equipments compute and exhibit the distributed private key which the inaccurate decode person has in cooperation with the case where an inaccurate person is specified as a means, a technical problem is solved by enabling it to calculate a right

result instead of the inaccurate decode person.

0022] The concrete means is as follows. n persons' decode person is set to $P1-Pn$, and the open value w_j of a proper is assigned to each decode person P_j . Threshold t which fills $3 \leq t \leq n$ is defined. (x_1, x_2, y_1, y_2, z) is distributed with the secrecy variational method of threshold t , and let the secrecy value (x_2, y_1, y_2, z) corresponding to a value w_j be the decode person's P_j private key.

0023] Moreover, let $X_j = g^{x_1} g^{x_2} \bmod p$, $Y_j = g^{y_1} g^{y_2} \bmod p$, and $Z_j = g^z \bmod p$ (X_j, Y_j, Z_j) be the decode person's P_j public keys. It considers as the public key which uses $1 \leq g \leq 2 \bmod p$ of $X = g, Y = g, Z = g$ for encryption. It shall connect by the safe channel between each decode person equipment, and each decode person equipment shall use the broadcast mold channel it is guaranteed to be to receive a content with other all the members' same decode person equipment.

0024] $E = (u_1, u_2, v, e)$ is made into the cipher of the plaintext m enciphered by the Cramer-Shoup code approach. Decode person equipment performs a distributed random-number generation procedure in cooperation, and the decode person's P_j equipment acquires the secrecy value j . Here, r_j is a secrecy value corresponding to the value w_j at the time of distributing random-number r with the secrecy variational method of threshold t , and is the value which can recover r with a secrecy decode procedure from the secrecy value of $t+1$ piece of arbitration. Moreover, each decode person cannot know the value of r , but r becomes the random integer of under or more $0q$ from the property of a distributed random-number generation procedure.

0025] Next, all decode person equipments cooperate, and perform a distributed multiplication means, and each decode person's P_j equipment obtains secrecy value $x_1', x_2', y_1',$ and y_2' . Secrecy value x_1' is a value which distributes the product of a random number r and a private key x_1 with the secrecy variational method of threshold t , and is acquired, and can decode x_1' to $r \cdot x_1 \bmod q$ which $t+1$ person's decode person of arbitration has here. r and $x_2 \bmod q, r \cdot y_1 \bmod q,$ and $r \cdot y_2 \bmod q$ can be similarly restored from the value of $t+1$ piece of arbitration about secrecy value $x_2', y_1',$ and y_2' , respectively.

0026] Each decode person P_j equipment which received E calculates $c = H(u_1, u_2)$ and $V_j = u_1 x_1' + c y_1' u_2 x_2' + c y_2' j' v - r_j \bmod p$, and transmits V_j to all other decode person equipments through a broadcast mold channel. Next, each decode person equipment checks that the exponent part of (V_1, \dots, V_n) is the codeword of a BCH code. When it becomes clear not the codeword of a BCH code but that it is not right, the exponent part of (V_1, \dots, V_n) each decode person's P_j equipment It proves to other decode persons by zero information certification, without leaking the information concerning [that V_j is as a result of / of $u_1 x_1' + c y_1' u_2 x_2' + c y_2' j' v - r_j \bmod p$ / count, and] $x_1', x_2', y_1', y_2',$ and r_j .

0027] It considers that the decode person P_j who failed in certification is an inaccurate person, and other decode person equipments recover secrecy value x_1' of the deviation person who is the inaccurate person, $x_2', y_1', y_2',$ and r_j using secrecy value recovery procedure, and he exhibits the value of the right V_j . The rights (V_1, \dots, V_n) including the value of the exhibited right V_j are obtained. After the exponent part of (V_1, \dots, V_n) checks the right thing and that it is a codeword, the secrecy restoration procedure to exponent part restores a value V . Each decode person equipment investigates whether V is equal to 1, and if not equal, decode will be refused and it will stop. [0028] If equal, each decode person's P_j equipment will calculate $D_j = u_1 z_j \bmod p$, and will transmit it to all other decode person equipments according to a broadcast mold channel. Each decode person equipment which received D_j verifies the codeword same with having carried out to (V_1, \dots, V_n) to (D_1, \dots, D_n) , when injustice is detected, performs zero information certification similarly, specifies an inaccurate person, and it recovers the value of the right D_j using secrecy value recovery procedure.

[0029] From the right (D_1, \dots, D_n) , with the secrecy restoration procedure to exponent part, each decode person equipment restores $D = u_1 z \bmod p$, calculates $m = e/D \bmod p$, and decodes Message m . the private key restoration procedure as opposed to [when each decode person equipment calculates according to the above-mentioned procedure] the exponent part from the right V_k of the arbitration beyond $2t+1$ piece -- $V = (u_1 x_1 + c y_1 u_2 x_2 + c y_2 v - 1) r \bmod p$ -- V can be restored. here, in cooperation with [V / V makes p law and] 1 -- if it becomes -- Cramer-Shoup -- in cooperation with [the original value of verification type $u_1 x_1 + c y_1 u_2 x_2 + c y_2$ in law] v . On the other hand, when V becomes in cooperation with 1, it is in cooperation with [an original verification type] v or a random number r is 0. However, the probabilities for the random number r generated in the distributed random-number generation procedure to be set to 0 are $1/q$, and since they are small enough, they can be disregarded. Therefore, V can consider in cooperation with [an original verification type] v , when in cooperation with 1.

[0030] Here, it is assumed that there are a maximum of t decode persons who commit injustice. these t persons -- (1) -- it is made for the value V of the verification type to the unjust cipher E to be set to 1 -- (2) -- it can deviate from the above-mentioned procedure for two kinds of the object of ** of making it the value V of the verification type to the just cipher E not set to 1 [or] However, the output of all decode person equipments can detect the existence, if an unjust value is less than [of the whole] $1/3$ when an unjust value exists since it is verified by codeword inspection of a BCH code. In such a case, since each decode person proves the rightness of an output value by zero information certification, the inaccurate person who outputted the unjust value fails in certification, and is eliminated.

[0031] About informational leakage, when V is not 1, since one value of r which fills $V = (u_1 x_1 + c y_1 u_2 x_2 + c y_2 v - 1) r \bmod p$ to any values of $u_1 x_1 + c y_1 u_2 x_2 + c y_2$ becomes settled, by the above-mentioned verification approach, the information about $u_1 x_1 + c y_1 u_2 x_2 + c y_2$ does not leak at all. As mentioned above, without leaking the information about a private key entirely, if the decode person who commits injustice according to this invention is less than [of all decode persons] $1/3$, by cooperation of two or more decode person, it is possible to calculate a verification type equivalent to the verification type of the original Cramer-Shoup code approach, and, therefore, two or more decode person's code decode approach strong against an accommodative selection cipher attack can be constituted.

[0032] By computing and exhibiting the distributed private key which codeword inspection of a BCH code is not conducted, but zero information certification is always performed in the above-mentioned means on the other hand, an inaccurate person is specified, other decode persons cooperate, and the inaccurate decode person has Although it also becomes bored, since a right result is calculable instead of the inaccurate decode person, it can respond to less than $1/2$ inaccurate person (in order to determine by majority that zero information certification is right, one half of decode persons at least must be right).

[0033]

[Embodiment of the Invention] The cipher verification approach which is the first example of this invention is explained to one or less example. The cipher created with cipher implementer equipment 11 as shown in drawing 1 is decoded with decode person equipment 12. If it is not a right cipher, in order to avoid carrying out decode refusal freely with decode person equipment 12, it verifies whether decode refusal is appropriate with verification person equipment 13.

[0034] There shall be the big prime factors p and q now, and q shall divide $p-1$. The origin g_1 and g_2 of G_q is chosen at random. It considers as the public key which uses $1 \leq g \leq 2 \bmod p$ of $X = g, Y = g, Z = g$ for an encryption procedure. Here, it is $(x_1,$

(x_2, y_1, y_2, z) Zq5. It carries out. The public key shall be exhibited with p, q, g_1 , and g_2 as a open parameter. Moreover, the private key shall be stored on the memory of decode person equipment.

[0035] As shown in drawing 2, after receiving cipher $E = (u_1, u_2, v, e)$ of the plaintext m enciphered by the Cramer-Shoup code approach which used X, Y , and Z as the public key (S1), Decode person equipment generates a random number r (S2), and calculates $c = H(u_1, u_2)$ and $v = (u_1 x_1 + c y_1 u_2 x_2 + c y_2 v - 1) r \bmod p$ (S3). If V becomes one, this cipher will be considered as acceptance and (S4) and decode count will be performed (S5).

[0036] If V is not 1, it will consider as a rejection. In order to prove that it is a rejection to a third party, $BC(r)$ is exhibited using bit commitment function $BC()$. There are some which are depended on Pedersen in this bit commitment function. That is, a random number s is generated and it calculates with $BC(r, s) = g^r h^s \bmod p$. dispersion of h to which g and h use g as a bottom here -- it is under G_q whose logarithm is strange.

[0037] r which constitutes $BC(r, s)$, x_1 which constitutes public keys X and Y , x_2 , and y_1 and y_2 -- using -- $r \bmod p (u_1 x_1 + c y_1 u_2 x_2 + c y_2 v - 1)$ -- it proves to a third party by zero information certification, without leaking the secrecy concerning [that the result of having calculated is V , and] r, x_1, x_2 , and y_1 and y_2 (S6). [then,] The following procedures perform this zero information certification.

[0038] dispersion of h which uses g as a bottom for g and h below -- it considers as the origin of G_q whose logarithm is strange. decode person equipment -- random numbers a, a_1, a_2, b_1 , and b_2 -- Zq -- choosing -- $R = g^r h^a \bmod p$, $RX_1 = R x_1 h a_1 \bmod p$, $RX_2 = R x_2 h a_2 \bmod p$, $RY_1 = R y_1 h b_1 \bmod p$, $RY_2 = R y_2 h b_2 \bmod p$ -- R, RX_1, RX_2, RY_1 , and RY_2 are sent to verification person equipment.

[0039] Furthermore, decode person equipment chooses a random number w_0 from Zq as random, and is $K = g$ and $L = g^{w_0} \bmod p$ is sent to verification person equipment. Verification person equipment calculates $B = K e_0 L e_1 \bmod p$ by choosing e_0 and e_1 from Zq as random, and sends B to decode person equipment.

[0040] Decode person equipment chooses random numbers w_1 - w_{18} from Zq as random. $T_1 = g_1 w_1 g_2 w_2 \bmod p$, $T_2 = g_1 w_3 g_2 w_4 \bmod p$, $T_3 = g w_5 g w_6 \bmod p$, $T_4 = R w_1 h w_7 \bmod p$, $T_5 = R w_2 h w_8 \bmod p$, $T_6 = R w_3 h w_9 \bmod p$, $T_7 = R w_4 h w_{10} \bmod p$, $T_8 = \text{Calculate } g w_{11} h w_{12} \bmod p$, $T_9 = g w_{13} h w_{14} \bmod p$, $T_{10} = g w_{15} h w_{16} \bmod p$, $T_{11} = g w_{17} h w_{18} \bmod p$, $T_{12} = u_1 w_{11} + c w_{15} u_2 w_{13} + c w_{17} v - w_5 \bmod p$. It sends to verification person equipment.

[0041] Verification person equipment sends e_0 and e_1 to decode person equipment.

Decode person equipment checks that $B = K e_0 L e_1 \bmod p$ is realized, and when not realized, it stops certification. When this is realized, Decode person equipment is $z_1 = w_1 + e_0$ and $x_1 \bmod q z_2 = w_2 + e_0$ and $x_2 \bmod q z_3 = w_3 + e_0$ and $y_1 \bmod q z_4 = w_4 + e_0$ and $y_2 \bmod q z_5 = w_5 + e_0$ and r . $\bmod q z_6 = w_6 + e_0$ and $\bmod q z_7 = w_7 + e_0$ and $a_1 \bmod q z_8 = w_8 + e_0$ and $a_2 \bmod q z_9 = w_9 + e_0$ and $b_1 \bmod q z_{10} = w_{10} + e_0$ and $b_2 \bmod q z_{11} = w_{11} + e_0$ and $r - x_1 \bmod q z_{12} = w_{12} + e_0$ ($a - x_1 + a_1$) $\bmod q z_{13} = w_{13} + e_0$, r , and $x_2 \bmod q z_{14} = w_{14} + e_0$ (a and $x_2 + a_2$) $\bmod q z_{15} = w_{15} + e_0$ and $r - y_1 \bmod q z_{16} = w_{16} + e_0$ ($a - y_1 + b_1$) $\bmod q z_{17} = w_{17} + e_0$ and $r - y_2 \bmod q z_{18} = w_{18} + e_0$ ($a - y_2 + b_2$) $\bmod q$. It calculates and z_1 - z_{18} , and w_0 are sent to verification person equipment.

[0042] Verification person equipment $L = g^{w_0} \bmod p$, $g_1 z_1 g_2 z_2 = T_1$, $X e_0 \bmod p$, $g_1 z_3 g_2 z_4 = T_2$, $Y e_0 \bmod p$, $g z_5 h z_6 = T_3$, $R e_0 \bmod p$, $R z_1 h z_7 = T_4$, $R e_0 \bmod p$, $R z_2 h z_8 = T_5$, $R e_0 \bmod p$, $R z_3 h z_9 = T_6$, $R e_0 \bmod p$, $R z_4 h z_{10} = T_7$, $R e_0 \bmod p$, $g z_{11} h z_{12} = T_8$, $R e_0 \bmod p$, $g z_{13} h z_{14} = T_9$, $R e_0 \bmod p$. It verifies that $g z_{15} h z_{16} = T_{10}$, $R e_0 \bmod p$, $g z_{17} h z_{18} = T_{11}$, $R e_0 \bmod p$. plutonium $z_{11} + c z_{15} u_2 z_{13} + c z_{17} v - z_5 = T_{12}$, $R e_0 \bmod p$ is realized.

[0043] The principle of the upper certification is Schnorr. It is the same as that of a signature, and since a verification type is realized only when decode person equipment creates correctly $V, X, Y, R, RX_1, RX_2, RY_1$, and RY_2 , when at least one is not realized, verification is considered as failure.

The second example of this invention is explained to two or less example. As shown in drawing 3 $R > 3$, they are code implementer equipment 11 and 121-12n of each equipment of the decode persons P_1 - P_n . It connects with the broadcast mold channel 14, and is 121-12n of decode person equipment. It connects by the channel 15 safe for mutual.

[0044] There shall be the big prime factors p and q now, and q shall divide $p-1$. The origin g_1 and g_2 of G_q is chosen at random. First, n persons' decode person is set to P_1 - P_n , and the open value w_j of a proper is assigned to each decode person P_j ($j = 1, 2, \dots, n$). Threshold t which fills $3 \leq t \leq n$ is defined. All decode person equipments perform the distributed random-number generation procedure of threshold t 3 times, and the decode person's P_j equipment acquires a secrecy value ($x_2 j$ and $y_1 j, y_2 x_1 j, j, z_j$), and makes this the decode person's P_j private key. Moreover, let $X_j = g_1 x_1 j g_2 x_2 j \bmod p$, $Y_j = g_1 y_1 j g_2 y_2 j \bmod p$, and $Z_j = g_1 z_j \bmod p$ (X_j, Y_j, Z_j) be the decode person's P_j public keys.

Furthermore, it considers as the public key which uses $1 x_1 g_2 x_2 \bmod p$ of $X = g, 1 y_1 g_2$ of $Y = g y_2 \bmod p$, and $Z = g_1 z \bmod p$ for an encryption procedure. Here, it is $((x_1, x_2, y_1, y_2, z)$ Zq5. It is the random number restored by the secrecy restoration procedure from $t+1$ set of secrecy values ($x_2 j$ and $y_1 j, y_2 x_1 j, j, z_j$) of arbitration. There is an approach by Pedersen in the distributed random-number generation procedure which generates such a random number. Below, the distributed random-number generation procedure is shown.

[0045] Between each decode person equipment, as shown in drawing 3, there shall be a safe channel 15 and each decode person equipment shall use the broadcast mold channel 14 it is guaranteed to be to receive a content with other all the members' same decode person equipment. S-1) the equipment of P_j -- two polynomials on Zq -- $f(X) = a_0 j + a_1 j X + \dots + a_t j X^t$ And $g_j(X) = b_0 j + b_1 j X + \dots + b_t j X^t$ random -- choosing -- every -- $f_j(w_k)$ and $g_j(w_k)$ are transmitted to the equipment except for $1, 2, \dots, n$, and $k = j$ $k = \dots$ of P_k through a safe channel.

[0046] S-2) The equipment of P_j calculates $C_{ij} = g_1 a_{ij} g_2 b_{ij} \bmod p$ to $i = 1, \dots, t$, and transmits it to all other decode person equipments through a broadcast mold channel.

S-3) The equipment of P_k which received C_{ij} from all other decode person equipments is $g_1 f_j(w_k) g_2 g_j(w_k) = C_0 j w_k$ and $C_1 j w_k$ as $w_k = w_k \bmod q$. -- It verifies that $C_{tj} w_k \bmod p$ is realized.

[0047] S-4) The equipment of P_k is $x_1 k = f_1(w_k) + f_2(w_k) + \dots$. They are $+f_n(w_k) \bmod q$ and $x_2 k = g_1(w_k) + g_2(w_k) + \dots$. Distributed random-number value $x_1 k$ and $x_2 k$ are obtained as $+g_n(w_k) \bmod q$.

S-5) $X = C_0, C_1$ -- It is referred to as $C_0 n \bmod p$. Private key $y_1 j, y_2 j$, and z_j to which public keys Y and Z and each decode person correspond similarly are also created similarly.

[0048] All decode person equipments generate distributed random-number r Zq with a distributed random-number generation procedure, and each decode person's P_j equipment holds the secrecy value r_j (drawing 5, S1). After receiving cipher $E = (u_1, u_2, v, e)$ of the plaintext m enciphered by the Cramer-Shoup code approach which used X, Y , and Z as the public key (S2), each decode person's P_j equipment calculates $c = H(u_1, u_2)$ and $V_j = (u_1 x_1 j + c y_1 j u_2 x_2 j + c y_2 j v - 1) r_j \bmod p$ (S3).

[0049] Then, the equipment of Pj distributes Vj with a threshold [of 2t] verifiable secrecy variational method, and the secrecy value Vjk corresponding to a value wk is transmitted through a channel safe for each decode person's Pk equipment (S4). The approach of Pedersen can be used for the verifiable secrecy variational method used here. The following is the procedure.

P-1) g and h which there are the big prime factors P and Q, and Q divides P-1, and are made into $Q > p$ are GQ whose value of $\log g h$ is strange. It considers as origin.

[0050] P-2) the equipment of Pj -- ZQ Two upper polynomials $f_j(X) = V_j + a_1 jX + \dots + a_t jX^t$ And $g_j(X) = b_0 j + b_1 jX + \dots + b_t jX^t$ (however, it considers as $a_0 j = V_j$) -- the part of Vj -- removing -- random -- choosing -- every -- $f_j(w_k)$ and $g_j(w_k)$, i.e., Vjk, are transmitted to the equipment of Pk through a safe channel.

P-3) The equipment of Pj calculates $C_{ij} = g_{a_{ij}} h_{b_{ij}} \bmod p$ to $i = 1, \dots, t$, and transmits it to all other decode person equipments through a broadcast mold channel.

[0051] P-4) The equipment of Pk which received C_{ij} is $g_{f_j}(w_k) h_{g_j}(w_k) = C_{0j} w_k^0$ and $C_{1j} w_k^1$ as $w_k = w_k \bmod q$. -- It verifies that $C_{tj} w_k^t \bmod q$ is realized, that is, Vjk is verified (S5).

P-5) When not realized, the equipment of Pk transmits a "rejection" to all other decode person equipments through a broadcast mold channel.

[0052] When advice of P-6 "a rejection" is $t+1$ or more pieces, it is considered that Pj is an inaccurate person, it is eliminated (S6), and all other decode person equipments discard all the information that the equipment of Pj transmitted before. The step of P-4, and 5 and 6 is the procedure of performing verification of the distributed secrecy value Vjk, and an inaccurate person's abatement, and after all decode person equipments finish transmitting data, you may carry out by releasing a rejection list collectively.

[0053] After all decode person equipments distribute Vj with the above-mentioned procedure, each decode person's Pj equipment transmits Vj and $b_0 j$ to all other decode person equipments through a broadcast mold channel (S7). The equipment of each decode person Pj who received this checks that $C_{0j} = g^{b_0 j} V_j h^{b_0 j} \bmod p$ is realized, and verifies Vj (S8). When not realized, like the above, a "rejection" is notified to all other decode person equipments, and an inaccurate person is eliminated (S9).

[0054] $2t+1$ piece is chosen as arbitration from the right and all checked $V_k(s)$ (S10), and it investigates whether the value V restored with the secrecy restoration procedure to exponent part is equal to 1 (S11). The secrecy restoration procedure to exponent part is reference. Cramer, et.al: "A secure and Optimally Efficient Multi-Authority Election Scheme", Advances in Cryptology-Eurocrypt'97, LNCS 1233 Springer-Verlag, pp.103-118, and 1997 It is detailed. The restoration procedure to the exponent part at the time of setting to alpha the set of the index k of $2t+1$ piece V_k chosen as below is shown. The secrecy value of exponent part presupposes that it is the secrecy value acquired with the verifiable secrecy variational method of Pedersen.

[0055] R-1) It is a Lagrange interpolation multiplier first [0056]

[Equation 1]

$$\lambda_{j, \alpha} = \prod_{k \in \alpha, k \neq j} j/(j-k)$$

It calculates by carrying out.

R-2) Next, [0057]

[Equation 2]

$$V = \prod_{j \in \alpha} V_j \lambda_{j, \alpha} \bmod p$$

It calculates. If V is not 1, a secrecy restoration procedure will be similarly repeated in other $2t+1$ piece combination (S12). If a restoration value is all equal to 1 about no combination, a rejection will be notified and it will stop.

[0058] If there is combination set to 1 at least one, this cipher will be considered as acceptance. Each decode person's Pj equipment calculates $D_j = u_1 z_j \bmod p$, as shown in drawing 4 R> 4 (S1), and it transmits it to all other decode person equipments according to a broadcast mold channel (S2). the dispersion to which each decode person equipment which received D_j uses u_1 of D_1, \dots, D_n as a bottom -- by checking that a logarithm is the codeword of a BCH code, if it is (S4) and a codeword, the secrecy restoration procedure to the above-mentioned exponent part will restore $D = u_1 z \bmod p$ (S5), $m = e/D \bmod p$ will be calculated, and Message m will be decoded (S6). If it is not a codeword in step S4, what is made to prove the rightness of count and cannot be proved by zero information certification will be discarded as inaccurate D_i (S7).

The third example of this invention is explained to three or less example.

[0059] A safe channel shall be between each decode person equipment, and each decode person equipment shall use the broadcast mold channel it is guaranteed to be to receive a content with other all the members' same decode person equipment. There shall be the big prime factors p and q and q shall divide p-1. The origin g_1 and g_2 of Gq is chosen at random. First, n persons' decode person is set to P_1-P_n , and the open value w_j of a proper is assigned to each decode person Pj. Threshold t which fills $3 \leq t < n$ is defined.

[0060] First, the secrecy distribution approach by Pedersen is shown. First, g and h It considers as the origin of Gq whose $\log g h$ is strange. The equipment of the portioner P who distributes the secrecy values a_0 and b_0 is t-th two polynomials $f(X) = a_0 + a_1 X + \dots$ on Z_q . -- It is $+atX^t$ and $g(X) = b_0 + b_1 X + \dots$ -- It is $+btX^t$. Except for a_0 , it chooses at random, and $f(w_j)$ and $g(w_j)$ are sent to each addressee's Pj equipment through a safe channel.

[0061] Next, the commitment value E_i of each multiplier is calculated like $E_i = g^{a_{i0}} h^{b_{i0}} \bmod p$ to $i = 0, \dots, t$, and it opens to the public through a broadcast mold channel. Each equipment of Pj which received these is $g^{f_j}(w_j)$ as $u_{ji} = w_{ji} \bmod q$. $h_{g_j}(w_j) = E_{0j} u_{j0} E_{1j} u_{j1}$ -- It verifies that $E_{tj} u_{jt} \bmod p$ is realized. This $E_{0j} u_{j0} E_{1j} u_{j1}$ -- The value of $E_{tj} u_{jt} \bmod p$ is called the commitment to the distributed secrecy value of Pj. If the commitment value of each multiplier is exhibited, anyone can also calculate the commitment to which distributed secrecy value of Pj.

[0062] Below, it is Ped (a_0, b_0) about this secrecy distribution approach [g, h]. -> ($a_0 j, b_0 j$) (E_0, \dots, E_t)

** -- it writes like. (a_0, b_0) are confidential information distributed, each equipment of Pj is the distributed secrecy value received through a safe channel, and its ($a_0 j, b_0 j$) are equal to $f(w_j)$ and $g(w_j)$ respectively. (E_0, \dots, E_t) are commitment values of each multiplier exhibited through a broadcast mold channel. [g, h] express the bottom used in case a commitment is created. As long as there is especially no notice about the above-mentioned notation, the multiplier of the polynomial except a constant term shall be chosen at random.

[0063] Thus, from the distributed secrecy value, when polynomial interpolation recovers the original secrecy, the holder of each distributed secrecy value exhibits the value first. It is $g^{a_0 j} h^{b_0 j} = E_{0j} u_{j0} E_{1j} u_{j1}$ to the exhibited value ($a_0 j, b_0 j$). -- It checks that $E_{tj} u_{jt} \bmod p$ is realized. The set which that index j makes is set to alpha about $t+1$ ($a_0 j, b_0 j$) of arbitration of which this formula consists. It is a Lagrange interpolation

multiplier [0064]

Equation 3]

$$\lambda_{i, \alpha} = \prod_{k \in \alpha, k \neq i} i/(i-k) \bmod q$$

t is [0065] when it carries out.

Equation 4]

$$\sum_{j \in \alpha} \lambda_{i, \alpha} a_{0j} \bmod q = a_0$$

A next door and a_0 are recoverable. b_0 is recoverable similarly. The above-mentioned secrecy distribution approach can completely be similarly performed, even if it uses only one bottom. In such a case, it is written as $\text{Ped}(a_0) [g] \rightarrow (a_0) (E_0, \dots, E_t)$.

[0066] The random number distributed in cooperation by two or more persons is generable using this secrecy distribution approach. First, the equipment of P_i chooses random numbers a_i and b_i from Z_q , and is this $\text{Ped}(a_i, b_i) [g, h] \rightarrow (a_{ij}, b_{ij}) (E_{i0}, \dots, E_{it})$

** -- it distributes like. All the members of P_1 - P_n perform this. Then, the equipment of P_j receives $(a_{1j}, b_{1j}), \dots, (a_{nj}, b_{nj})$ from a safe channel, and receives $(E_{10}, \dots, E_{1t}), \dots, (E_{n0}, \dots, E_{nt})$ from a broadcast mold channel. At this time, it is the distributed secrecy value (x_{1j}, x_{2j}) of P_j $x_{1j} = a_{1j} + \dots + a_{nj} \bmod q$, $x_{2j} = b_{1j} + \dots + b_{nj} \bmod q$. It is referred to as $+b_{nj} \bmod q$. The random-number value x_1 recovered from this distributed secrecy value is [0067].

Equation 5]

$$x_1 = \sum_{j \in \alpha} \lambda_{k, \alpha} x_{1j} = a_1 + \dots + a_n \bmod q$$

The value is known by nobody until it comes out, and it is and recovery is performed. Moreover, the commitment value EX_k of the k -th multiplier of the polynomial which makes this secrecy random-number value a constant serves as $EX_k = E_1 k - E_2 k - \dots - E_{nk} \bmod p$. Especially, it is cautious of it being $EX_0 = g x_1 h x_2 \bmod p$. This approach is called distributed random-number generation, and it is $\text{Rand}([a], [b]) [g, h] \rightarrow (a_j, b_j) (E_0, \dots, E_t)$.

It writes. $([a] [b])$ is a random-number value generated and means that the value of $[]$ is strange to every calculator. $[g, h] --$ and $[]$ of semantics $(a_j, b_j) (E_0, \dots, E_t)$ is the same as that of the notation of the above-mentioned secrecy distribution.

[0068] All decode person equipments are the distributed random-number generation procedure of threshold t $\text{Rand}([x_1], [x_2]) [g_1, g_2] \rightarrow (x_{1j}, x_{2j}) (EX_0, \dots, EX_t)$

$\text{Rand}([y_1], [y_2]) [g_1, g_2] \rightarrow (y_{1j}, y_{2j}) (EY_0, \dots, EY_t)$

$\text{Rand}([z_1]) [g_1] \rightarrow (z_{1j}) (EZ_0, \dots, EZ_t)$

** -- performing 3 times like, the decode person P_j acquires a secrecy value $(x_{2j}$ and $y_{1j}, y_{2j}, x_{1j}, z_{1j})$, and makes this the decode person's P_j private key. Moreover, let $X_j = g x_{1j} g_2 x_{2j} \bmod p$, $Y_j = g y_{1j} g_2 y_{2j} \bmod p$, and $Z_j = g z_{1j} \bmod p$ (X_j, Y_j, Z_j) be the decode person's P_j public keys. Furthermore, it considers as the public key which uses $X = EX_0 = g x_1 g_2 x_2 \bmod p$, $Y = EY_0 = g y_1 g_2 y_2 \bmod p$, and $Z = EZ_0 = g z_1 \bmod p$ for an encryption procedure. It is $*(x_1, x_2, y_1, y_2, z) Z_q^5$ here. It is the random number restored by the secrecy restoration procedure from $t+1$ set of secrecy values $(x_{2j}$ and $y_{1j}, y_{2j}, x_{1j}, z_{1j})$ of arbitration.

[0069] All decode person equipments perform distributed random-number generation procedure $\text{Rand}([r], [s]) [g_1, g_2] \rightarrow (r_j, s_j) (R_0, \dots, R_t)$, and generate distributed random-number $r^{**} Z_q$, and each decode person's P_j equipment holds the secrecy values r_j and s_j (drawing 6, S_1). R is set to $R = R_0 = g_1 r g_2 \bmod p$ here.

[0070] Next, all decode person equipments obtain secrecy value $x_{1j}', x_{2j}', y_{1j}',$ and y_{2j}' with a distributed multiplication means (S_2). Secrecy value x_{1j}' is a value which distributes the product of a random number r and a private key x_1 with the secrecy variational method of threshold t , and is acquired, and can decode $r x_1 \bmod q$ here from x_{1j}' which $t+1$ person's decode person of arbitration has. $r x_2 \bmod q$, $r y_1 \bmod q$, and $r y_2 \bmod q$ can be similarly restored from the value of $t+1$ piece of arbitration about secrecy value $x_{2j}', y_{1j}',$ and y_{2j}' , respectively. About such a distributed multiplication means, it performs as follows.

[0071] The decode person's P_j equipment is $\text{Ped}(x_{1j}, x_{2j}) [g_1, g_2] \rightarrow (x_{1ji}, x_{2ji}) (EX_{j0}, \dots, EX_{jt})$.

It performs. Each equipment of P_j calculates $R_j = g_1 r_j g_2 s_j \bmod p$. This value R_j is $R_j = R_0 u_j$ as $u_j = w_j \bmod q$. -- Since you may calculate like $R_{t+j} \bmod p$, it is cautious of the ability of anyone to calculate.

[0072] Next, the polynomial used for distributing x_{1j} and x_{2j} by $\text{Ped}(x_{1j}, x_{2j})$ is used for the equipment of P_j as it is, and it is $\text{Ped}(x_{1j}, s_{1j})$

$[R_j, g_2] \rightarrow (x_{1ji}, s_{1ji}) (ERX_{1j0}, \dots, ERX_{1jt})$.

$\text{Ped}(x_{2j}, s_{2j}) [R_j, g_2] \rightarrow (x_{2ji}, s_{2ji}) (ERX_{2j0}, \dots, ERX_{2jt})$

It performs. However, s_{1j} and s_{2j} also choose at random the polynomial which chooses at random and makes these a constant term.

[0073] To the last, the equipment of P_j is $\text{Ped}(x_{1j} - r_j, x_{1j} - s_j + s_{1j}) [g_1, g_2] \rightarrow (rx_{1ji}, rs_{1ji}) (ERX_{1j0}, \dots, ERX_{1jt})$.

$\text{Ped}(x_{2j} - r_j, x_{2j} - s_j + s_{2j}) [g_1, g_2] \rightarrow (rx_{2ji}, rs_{2ji}) (ERX_{2j0}, \dots, ERX_{2jt})$

It carries out.

[0074] Each equipment of P_1 - P_n performs the above-mentioned procedure. The equipment of P_i is the set $(rx_{1li}, \dots, rx_{1ni})$ of a distributed secrecy value which received to a Lagrange interpolation multiplier [0075]

Equation 6]

$$\lambda_{j, \alpha} = \prod_{k \in \alpha, k \neq j} j/(j-k) \text{ として、}$$

$$x_{1j}' = \sum_{j \in \alpha} \lambda_{j, \alpha} r x_{1ji} \bmod q$$

It calculates. The set of the index of right x_{1j}' is set to β , and it is [0076] at the time of $|\beta| \geq t+1$.

Equation 7]

$$\begin{aligned} \sum_{j \in \beta} \lambda_{j, \beta} x_{1j}' &= \sum_{j \in \beta} \{ \lambda_{j, \beta} \sum_{i \in \alpha} \lambda_{i, \alpha} r x_{1i} \} \\ &= \sum_{i \in \alpha} \lambda_{i, \alpha} \{ \sum_{j \in \beta} \lambda_{j, \beta} r x_{1i} \} \\ &= \sum_{i \in \alpha} \lambda_{i, \alpha} r i \cdot x_{1i} = r \cdot x_1 \end{aligned}$$

since a next door and multiplication result $r \cdot x_1$ are recoverable, it turns out that x_{1j}' is the t -th distributed secrecy value of $r \cdot x_1$. x_{2j}' as well as y_{1j}' is calculated. Furthermore, a distributed multiplication procedure is similarly performed and calculated about secrecy value y_{1j}' and y_{2j}' . [0077] After receiving cipher $E = (u_1, u_2, v, e)$ to the plaintext m enciphered by the Cramer-Shoup code approach (S3), each decode person's P_j equipment $c = H(u_1, u_2)$ and $V_j = u_1 x_{1j}' + c y_{1j}' u_{2x_{2j}'} + c y_{2j}' v - r_j \bmod p$ are calculated, and V_j is transmitted to all other decode person equipments through (S4) and a broadcast mold channel (S5). Next, as for each decode person equipment, the exponent part of (V_1, \dots, V_n) checks that it is the codeword of a BCH code (S6). A codeword verification procedure reference F.J. MacWilliams : "The Theory of Error Correcting Codes", North-Holland Mathematical Library, and pp.201-202 -- or M. Ben-Or and S. Goldwasser, A. Wigerson : "Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation" and 20 th ACM Symposium on Theory of Computing, pp.1-10, and 1988. A codeword verification procedure is shown below.

$w! = 1$ is used as the n -th root of 1 in mod q , and it is referred to as $x_{iij} = w^j (i-1) \bmod q$.

It is [0078] about $j = 1, \dots, \text{all } 2t_j$.

Equation 8]

$$\sqrt[1]{x_{1j}} \sqrt[2]{x_{2j}} \dots \sqrt[n]{x_{nj}} \bmod p = 1$$

It checks becoming. When it becomes clear with the above-mentioned procedure that the exponent part of (V_1, \dots, V_n) is not right, each decode person's P_j equipment It proves to other decode person equipments by zero information certification, without leaking the information concerning [that V_j is as a result of / of $u_1 x_{1j}' + c y_{1j}' u_{2x_{2j}'} + c y_{2j}' v - r_j \bmod p$ / count, and] x_{1j}' , x_{2j}' , y_{1j}' , y_{2j}' , and r_j (S7).

[0079] This zero information certification is performed as follows. However, by explanation of the procedure to following P_j , since Subscript j is attached to all variables, this is excluded and explained. First, distributed secrecy value x_1' which P_j holds, x_2' , y_1' , y_2' , and r are received. a, u_1, a_2 , and b_1 as a certain random number $R = g^{1r} g^{2\text{second}} \bmod p$ $RX_1 = ERX_{10} = R x_{1g2a1} \bmod p$ $RX_2 = ERX_{20} = R x_{2g2a2} \bmod p$ $RY_1 = ERY_{10} = R y_{1g2b1} \bmod p$ $RY_2 = ERY_{20} = R y_{2g2b2} \bmod p$ The values R, RX_1, RX_2, RY_1 , and RY_2 of a commitment p Becoming can be acquired from the commitment value of the multiplier exhibited with the distributed random-number generation means and the distributed multiplication means to anyone.

[0080] P_j chooses a random number w_0 from Z_q as random, and sends $K = g$ and $L = g w_0 \bmod p$ to other decode person equipments. Other decode person equipments cooperate and are $\text{Rand}([e_0], [e_1]) [K, L] \rightarrow (e_{0i}, e_{1i}) (Ee_0, \dots, Ee_t)$. It performs and $Ee_0 = K e_0 L e_1 \bmod p$ is sent to the equipment of P_j .

[0081] The equipment of P_j chooses random numbers $w_1 - w_{18}$ from Z_q as random. $T_1 = g^{1w_1} g^{2w_2} \bmod p$ $T_2 = g^{1w_3} g^{2w_4} \bmod p$ $T_3 = g^{1w_5} g^{2w_6} \bmod p$ $T_4 = R w_1 h w_7 \bmod p$ $T_5 = R w_2 h w_8 \bmod p$ $T_6 = R w_3 h w_9 \bmod p$ $T_7 = R w_4 h w_{10} \bmod p$ $T_8 = \text{Calculate } g^{w_{11}} h^{w_{12}} \bmod p$ $T_9 = g^{w_{13}} h^{w_{14}} \bmod p$ $T_{10} = g^{w_{15}} h^{w_{16}} \bmod p$ $T_{11} = g^{w_{17}} h^{w_{18}} \bmod p$ $T_{12} = u_1 w_{11} + c w_{15} u_2 w_{13} + c w_{17} v - w_5 \bmod p$. It sends to other decode person equipments.

[0082] Other decode person equipments exhibit a distributed secrecy value, recover e_0 and e_1 , and send them to the equipment of P_j . The equipment of P_j checks that $Ee_0 = K e_0 L e_1 \bmod p$ is realized, and when not realized, it stops certification. When this is realized, The equipment of P_j $S_1 = w_1 + e_0$ and $x_1 \bmod q$ $S_2 = w_2 + e_0 \bmod q$ $S_3 = w_3 + e_0 \bmod q$ $S_4 = w_4 + e_0 \bmod q$ $S_5 = w_5 + e_0 \bmod q$ $S_6 = w_6 + e_0 \bmod q$ $S_7 = w_7 + e_0 \bmod q$ $S_8 = w_8 + e_0 \bmod q$ $S_9 = w_9 + e_0 \bmod q$ $S_{10} = w_{10} + e_0 \bmod q$ $S_{11} = w_{11} + e_0 \bmod q$ $S_{12} = w_{12} + e_0 \bmod q$ $S_{13} = w_{13} + e_0 \bmod q$, r , and $x_2 \bmod q$ $S_{14} = w_{14} + e_0 (a \text{ and } x_2 + a_2) \bmod q$ $S_{15} = w_{15} + e_0 \bmod q$ and $r - y_1 \bmod q$ $S_{16} = w_{16} + e_0 (a - y_1 + b_1) \bmod q$ $S_{17} = w_{17} + e_0 \bmod q$ and $r - y_2 \bmod q$ $S_{18} = w_{18} + e_0 (a - y_2 + b_2) \bmod q$ is calculated, and $S_1 - S_{18}$, and w_0 are sent to other decode person equipments. Other decode person equipments $L = g^{w_0} \bmod p$ One s_1 of $pg(s)$ 2 One s_3 of $s_2 = T_1 X e_0 \bmod pg(s)$ 2 $s_4 = T_2 Y e_0 \bmod pg(s)$ $s_5 = T_3 R e_0 \bmod pg(s)$ $s_6 = T_4 e(RX_1) \bmod pg(s)$ $s_7 = T_5 e(RX_2) \bmod pg(s)$ $s_8 = T_6 e(RY_1) \bmod pg(s)$ $s_9 = T_7 e(RY_2) \bmod pg(s)$ $s_{10} = T_8 e(RX_1) \bmod pg(s)$ $s_{11} = T_9 e(RX_2) \bmod pg(s)$ $s_{12} = T_{10} e(RY_1) \bmod pg(s)$ $s_{13} = T_{11} e(RY_2) \bmod pg(s)$ $s_{14} = T_{12} e(RX_1) \bmod pg(s)$ $s_{15} = T_{13} e(RX_2) \bmod pg(s)$ $s_{16} = T_{14} e(RY_1) \bmod pg(s)$ $s_{17} = T_{15} e(RY_2) \bmod pg(s)$ $s_{18} = T_{16} e(RX_1) \bmod pg(s)$ $s_{19} = T_{17} e(RX_2) \bmod pg(s)$ $s_{20} = T_{18} e(RY_1) \bmod pg(s)$ $s_{21} = T_{19} e(RY_2) \bmod pg(s)$ $s_{22} = T_{20} e(RX_1) \bmod pg(s)$ $s_{23} = T_{21} e(RX_2) \bmod pg(s)$ $s_{24} = T_{22} e(RY_1) \bmod pg(s)$ $s_{25} = T_{23} e(RY_2) \bmod pg(s)$ $s_{26} = T_{24} e(RX_1) \bmod pg(s)$ $s_{27} = T_{25} e(RX_2) \bmod pg(s)$ $s_{28} = T_{26} e(RY_1) \bmod pg(s)$ $s_{29} = T_{27} e(RY_2) \bmod pg(s)$ $s_{30} = T_{28} e(RX_1) \bmod pg(s)$ $s_{31} = T_{29} e(RX_2) \bmod pg(s)$ $s_{32} = T_{30} e(RY_1) \bmod pg(s)$ $s_{33} = T_{31} e(RY_2) \bmod pg(s)$ $s_{34} = T_{32} e(RX_1) \bmod pg(s)$ $s_{35} = T_{33} e(RX_2) \bmod pg(s)$ $s_{36} = T_{34} e(RY_1) \bmod pg(s)$ $s_{37} = T_{35} e(RY_2) \bmod pg(s)$ $s_{38} = T_{36} e(RX_1) \bmod pg(s)$ $s_{39} = T_{37} e(RX_2) \bmod pg(s)$ $s_{40} = T_{38} e(RY_1) \bmod pg(s)$ $s_{41} = T_{39} e(RY_2) \bmod pg(s)$ $s_{42} = T_{40} e(RX_1) \bmod pg(s)$ $s_{43} = T_{41} e(RX_2) \bmod pg(s)$ $s_{44} = T_{42} e(RY_1) \bmod pg(s)$ $s_{45} = T_{43} e(RY_2) \bmod pg(s)$ $s_{46} = T_{44} e(RX_1) \bmod pg(s)$ $s_{47} = T_{45} e(RX_2) \bmod pg(s)$ $s_{48} = T_{46} e(RY_1) \bmod pg(s)$ $s_{49} = T_{47} e(RY_2) \bmod pg(s)$ $s_{50} = T_{48} e(RX_1) \bmod pg(s)$ $s_{51} = T_{49} e(RX_2) \bmod pg(s)$ $s_{52} = T_{50} e(RY_1) \bmod pg(s)$ $s_{53} = T_{51} e(RY_2) \bmod pg(s)$ $s_{54} = T_{52} e(RX_1) \bmod pg(s)$ $s_{55} = T_{53} e(RX_2) \bmod pg(s)$ $s_{56} = T_{54} e(RY_1) \bmod pg(s)$ $s_{57} = T_{55} e(RY_2) \bmod pg(s)$ $s_{58} = T_{56} e(RX_1) \bmod pg(s)$ $s_{59} = T_{57} e(RX_2) \bmod pg(s)$ $s_{60} = T_{58} e(RY_1) \bmod pg(s)$ $s_{61} = T_{59} e(RY_2) \bmod pg(s)$ $s_{62} = T_{60} e(RX_1) \bmod pg(s)$ $s_{63} = T_{61} e(RX_2) \bmod pg(s)$ $s_{64} = T_{62} e(RY_1) \bmod pg(s)$ $s_{65} = T_{63} e(RY_2) \bmod pg(s)$ $s_{66} = T_{64} e(RX_1) \bmod pg(s)$ $s_{67} = T_{65} e(RX_2) \bmod pg(s)$ $s_{68} = T_{66} e(RY_1) \bmod pg(s)$ $s_{69} = T_{67} e(RY_2) \bmod pg(s)$ $s_{70} = T_{68} e(RX_1) \bmod pg(s)$ $s_{71} = T_{69} e(RX_2) \bmod pg(s)$ $s_{72} = T_{70} e(RY_1) \bmod pg(s)$ $s_{73} = T_{71} e(RY_2) \bmod pg(s)$ $s_{74} = T_{72} e(RX_1) \bmod pg(s)$ $s_{75} = T_{73} e(RX_2) \bmod pg(s)$ $s_{76} = T_{74} e(RY_1) \bmod pg(s)$ $s_{77} = T_{75} e(RY_2) \bmod pg(s)$ $s_{78} = T_{76} e(RX_1) \bmod pg(s)$ $s_{79} = T_{77} e(RX_2) \bmod pg(s)$ $s_{80} = T_{78} e(RY_1) \bmod pg(s)$ $s_{81} = T_{79} e(RY_2) \bmod pg(s)$ $s_{82} = T_{80} e(RX_1) \bmod pg(s)$ $s_{83} = T_{81} e(RX_2) \bmod pg(s)$ $s_{84} = T_{82} e(RY_1) \bmod pg(s)$ $s_{85} = T_{83} e(RY_2) \bmod pg(s)$ $s_{86} = T_{84} e(RX_1) \bmod pg(s)$ $s_{87} = T_{85} e(RX_2) \bmod pg(s)$ $s_{88} = T_{86} e(RY_1) \bmod pg(s)$ $s_{89} = T_{87} e(RY_2) \bmod pg(s)$ $s_{90} = T_{88} e(RX_1) \bmod pg(s)$ $s_{91} = T_{89} e(RX_2) \bmod pg(s)$ $s_{92} = T_{90} e(RY_1) \bmod pg(s)$ $s_{93} = T_{91} e(RY_2) \bmod pg(s)$ $s_{94} = T_{92} e(RX_1) \bmod pg(s)$ $s_{95} = T_{93} e(RX_2) \bmod pg(s)$ $s_{96} = T_{94} e(RY_1) \bmod pg(s)$ $s_{97} = T_{95} e(RY_2) \bmod pg(s)$ $s_{98} = T_{96} e(RX_1) \bmod pg(s)$ $s_{99} = T_{97} e(RX_2) \bmod pg(s)$ $s_{100} = T_{98} e(RY_1) \bmod pg(s)$ $s_{101} = T_{99} e(RY_2) \bmod pg(s)$ $s_{102} = T_{100} e(RX_1) \bmod pg(s)$ $s_{103} = T_{101} e(RX_2) \bmod pg(s)$ $s_{104} = T_{102} e(RY_1) \bmod pg(s)$ $s_{105} = T_{103} e(RY_2) \bmod pg(s)$ $s_{106} = T_{104} e(RX_1) \bmod pg(s)$ $s_{107} = T_{105} e(RX_2) \bmod pg(s)$ $s_{108} = T_{106} e(RY_1) \bmod pg(s)$ $s_{109} = T_{107} e(RY_2) \bmod pg(s)$ $s_{110} = T_{108} e(RX_1) \bmod pg(s)$ $s_{111} = T_{109} e(RX_2) \bmod pg(s)$ $s_{112} = T_{110} e(RY_1) \bmod pg(s)$ $s_{113} = T_{111} e(RY_2) \bmod pg(s)$ $s_{114} = T_{112} e(RX_1) \bmod pg(s)$ $s_{115} = T_{113} e(RX_2) \bmod pg(s)$ $s_{116} = T_{114} e(RY_1) \bmod pg(s)$ $s_{117} = T_{115} e(RY_2) \bmod pg(s)$ $s_{118} = T_{116} e(RX_1) \bmod pg(s)$ $s_{119} = T_{117} e(RX_2) \bmod pg(s)$ $s_{120} = T_{118} e(RY_1) \bmod pg(s)$ $s_{121} = T_{119} e(RY_2) \bmod pg(s)$ $s_{122} = T_{120} e(RX_1) \bmod pg(s)$ $s_{123} = T_{121} e(RX_2) \bmod pg(s)$ $s_{124} = T_{122} e(RY_1) \bmod pg(s)$ $s_{125} = T_{123} e(RY_2) \bmod pg(s)$ $s_{126} = T_{124} e(RX_1) \bmod pg(s)$ $s_{127} = T_{125} e(RX_2) \bmod pg(s)$ $s_{128} = T_{126} e(RY_1) \bmod pg(s)$ $s_{129} = T_{127} e(RY_2) \bmod pg(s)$ $s_{130} = T_{128} e(RX_1) \bmod pg(s)$ $s_{131} = T_{129} e(RX_2) \bmod pg(s)$ $s_{132} = T_{130} e(RY_1) \bmod pg(s)$ $s_{133} = T_{131} e(RY_2) \bmod pg(s)$ $s_{134} = T_{132} e(RX_1) \bmod pg(s)$ $s_{135} = T_{133} e(RX_2) \bmod pg(s)$ $s_{136} = T_{134} e(RY_1) \bmod pg(s)$ $s_{137} = T_{135} e(RY_2) \bmod pg(s)$ $s_{138} = T_{136} e(RX_1) \bmod pg(s)$ $s_{139} = T_{137} e(RX_2) \bmod pg(s)$ $s_{140} = T_{138} e(RY_1) \bmod pg(s)$ $s_{141} = T_{139} e(RY_2) \bmod pg(s)$ $s_{142} = T_{140} e(RX_1) \bmod pg(s)$ $s_{143} = T_{141} e(RX_2) \bmod pg(s)$ $s_{144} = T_{142} e(RY_1) \bmod pg(s)$ $s_{145} = T_{143} e(RY_2) \bmod pg(s)$ $s_{146} = T_{144} e(RX_1) \bmod pg(s)$ $s_{147} = T_{145} e(RX_2) \bmod pg(s)$ $s_{148} = T_{146} e(RY_1) \bmod pg(s)$ $s_{149} = T_{147} e(RY_2) \bmod pg(s)$ $s_{150} = T_{148} e(RX_1) \bmod pg(s)$ $s_{151} = T_{149} e(RX_2) \bmod pg(s)$ $s_{152} = T_{150} e(RY_1) \bmod pg(s)$ $s_{153} = T_{151} e(RY_2) \bmod pg(s)$ $s_{154} = T_{152} e(RX_1) \bmod pg(s)$ $s_{155} = T_{153} e(RX_2) \bmod pg(s)$ $s_{156} = T_{154} e(RY_1) \bmod pg(s)$ $s_{157} = T_{155} e(RY_2) \bmod pg(s)$ $s_{158} = T_{156} e(RX_1) \bmod pg(s)$ $s_{159} = T_{157} e(RX_2) \bmod pg(s)$ $s_{160} = T_{158} e(RY_1) \bmod pg(s)$ $s_{161} = T_{159} e(RY_2) \bmod pg(s)$ $s_{162} = T_{160} e(RX_1) \bmod pg(s)$ $s_{163} = T_{161} e(RX_2) \bmod pg(s)$ $s_{164} = T_{162} e(RY_1) \bmod pg(s)$ $s_{165} = T_{163} e(RY_2) \bmod pg(s)$ $s_{166} = T_{164} e(RX_1) \bmod pg(s)$ $s_{167} = T_{165} e(RX_2) \bmod pg(s)$ $s_{168} = T_{166} e(RY_1) \bmod pg(s)$ $s_{169} = T_{167} e(RY_2) \bmod pg(s)$ $s_{170} = T_{168} e(RX_1) \bmod pg(s)$ $s_{171} = T_{169} e(RX_2) \bmod pg(s)$ $s_{172} = T_{170} e(RY_1) \bmod pg(s)$ $s_{173} = T_{171} e(RY_2) \bmod pg(s)$ $s_{174} = T_{172} e(RX_1) \bmod pg(s)$ $s_{175} = T_{173} e(RX_2) \bmod pg(s)$ $s_{176} = T_{174} e(RY_1) \bmod pg(s)$ $s_{177} = T_{175} e(RY_2) \bmod pg(s)$ $s_{178} = T_{176} e(RX_1) \bmod pg(s)$ $s_{179} = T_{177} e(RX_2) \bmod pg(s)$ $s_{180} = T_{178} e(RY_1) \bmod pg(s)$ $s_{181} = T_{179} e(RY_2) \bmod pg(s)$ $s_{182} = T_{180} e(RX_1) \bmod pg(s)$ $s_{183} = T_{181} e(RX_2) \bmod pg(s)$ $s_{184} = T_{182} e(RY_1) \bmod pg(s)$ $s_{185} = T_{183} e(RY_2) \bmod pg(s)$ $s_{186} = T_{184} e(RX_1) \bmod pg(s)$ $s_{187} = T_{185} e(RX_2) \bmod pg(s)$ $s_{188} = T_{186} e(RY_1) \bmod pg(s)$ $s_{189} = T_{187} e(RY_2) \bmod pg(s)$ $s_{190} = T_{188} e(RX_1) \bmod pg(s)$ $s_{191} = T_{189} e(RX_2) \bmod pg(s)$ $s_{192} = T_{190} e(RY_1) \bmod pg(s)$ $s_{193} = T_{191} e(RY_2) \bmod pg(s)$ $s_{194} = T_{192} e(RX_1) \bmod pg(s)$ $s_{195} = T_{193} e(RX_2) \bmod pg(s)$ $s_{196} = T_{194} e(RY_1) \bmod pg(s)$ $s_{197} = T_{195} e(RY_2) \bmod pg(s)$ $s_{198} = T_{196} e(RX_1) \bmod pg(s)$ $s_{199} = T_{197} e(RX_2) \bmod pg(s)$ $s_{200} = T_{198} e(RY_1) \bmod pg(s)$ $s_{201} = T_{199} e(RY_2) \bmod pg(s)$ $s_{202} = T_{200} e(RX_1) \bmod pg(s)$ $s_{203} = T_{201} e(RX_2) \bmod pg(s)$ $s_{204} = T_{202} e(RY_1) \bmod pg(s)$ $s_{205} = T_{203} e(RY_2) \bmod pg(s)$ $s_{206} = T_{204} e(RX_1) \bmod pg(s)$ $s_{207} = T_{205} e(RX_2) \bmod pg(s)$ $s_{208} = T_{206} e(RY_1) \bmod pg(s)$ $s_{209} = T_{207} e(RY_2) \bmod pg(s)$ $s_{210} = T_{208} e(RX_1) \bmod pg(s)$ $s_{211} = T_{209} e(RX_2) \bmod pg(s)$ $s_{212} = T_{210} e(RY_1) \bmod pg(s)$ $s_{213} = T_{211} e(RY_2) \bmod pg(s)$ $s_{214} = T_{212} e(RX_1) \bmod pg(s)$ $s_{215} = T_{213} e(RX_2) \bmod pg(s)$ $s_{216} = T_{214} e(RY_1) \bmod pg(s)$ $s_{217} = T_{215} e(RY_2) \bmod pg(s)$ $s_{218} = T_{216} e(RX_1) \bmod pg(s)$ $s_{219} = T_{217} e(RX_2) \bmod pg(s)$ $s_{220} = T_{218} e(RY_1) \bmod pg(s)$ $s_{221} = T_{219} e(RY_2) \bmod pg(s)$ $s_{222} = T_{220} e(RX_1) \bmod pg(s)$ $s_{223} = T_{221} e(RX_2) \bmod pg(s)$ $s_{224} = T_{222} e(RY_1) \bmod pg(s)$ $s_{225} = T_{223} e(RY_2) \bmod pg(s)$ $s_{226} = T_{224} e(RX_1) \bmod pg(s)$ $s_{227} = T_{225} e(RX_2) \bmod pg(s)$ $s_{228} = T_{226} e(RY_1) \bmod pg(s)$ $s_{229} = T_{227} e(RY_2) \bmod pg(s)$ $s_{230} = T_{228} e(RX_1) \bmod pg(s)$ $s_{231} = T_{229} e(RX_2) \bmod pg(s)$ $s_{232} = T_{230} e(RY_1) \bmod pg(s)$ $s_{233} = T_{231} e(RY_2) \bmod pg(s)$ $s_{234} = T_{232} e(RX_1) \bmod pg(s)$ $s_{235} = T_{233} e(RX_2) \bmod pg(s)$ $s_{236} = T_{234} e(RY_1) \bmod pg(s)$ $s_{237} = T_{235} e(RY_2) \bmod pg(s)$ $s_{238} = T_{236} e(RX_1) \bmod pg(s)$ $s_{239} = T_{237} e(RX_2) \bmod pg(s)$ $s_{240} = T_{238} e(RY_1) \bmod pg(s)$ $s_{241} = T_{239} e(RY_2) \bmod pg(s)$ $s_{242} = T_{240} e(RX_1) \bmod pg(s)$ $s_{243} = T_{241} e(RX_2) \bmod pg(s)$ $s_{244} = T_{242} e(RY_1) \bmod pg(s)$ $s_{245} = T_{243} e(RY_2) \bmod pg(s)$ $s_{246} = T_{244} e(RX_1) \bmod pg(s)$ $s_{247} = T_{245} e(RX_2) \bmod pg(s)$ $s_{248} = T_{246} e(RY_1) \bmod pg(s)$ $s_{249} = T_{247} e(RY_2) \bmod pg(s)$ $s_{250} = T_{248} e(RX_1) \bmod pg(s)$ $s_{251} = T_{249} e(RX_2) \bmod pg(s)$ $s_{252} = T_{250} e(RY_1) \bmod pg(s)$ $s_{253} = T_{251} e(RY_2) \bmod pg(s)$ $s_{254} = T_{252} e(RX_1) \bmod pg(s)$ $s_{255} = T_{253} e(RX_2) \bmod pg(s)$ $s_{256} = T_{254} e(RY_1) \bmod pg(s)$ $s_{257} = T_{255} e(RY_2) \bmod pg(s)$ $s_{258} = T_{256} e(RX_1) \bmod pg(s)$ $s_{259} = T_{257} e(RX_2) \bmod pg(s)$ $s_{260} = T_{258} e(RY_1) \bmod pg(s)$ $s_{261} = T_{259} e(RY_2) \bmod pg(s)$ $s_{262} = T_{260} e(RX_1) \bmod pg(s)$ $s_{263} = T_{261} e(RX_2) \bmod pg(s)$ $s_{264} = T_{262} e(RY_1) \bmod pg(s)$ $s_{265} = T_{263} e(RY_2) \bmod pg(s)$ $s_{266} = T_{264} e(RX_1) \bmod pg(s)$ $s_{267} = T_{265} e(RX_2) \bmod pg(s)$ $s_{268} = T_{266} e(RY_1) \bmod pg(s)$ $s_{269} = T_{267} e(RY_2) \bmod pg(s)$ $s_{270} = T_{268} e(RX_1) \bmod pg(s)$ $s_{271} = T_{269} e(RX_2) \bmod pg(s)$ $s_{272} = T_{270} e(RY_1) \bmod pg(s)$ $s_{273} = T_{271} e(RY_2) \bmod pg(s)$ $s_{274} = T_{272} e(RX_1) \bmod pg(s)$ $s_{275} = T_{273} e(RX_2) \bmod pg(s)$ $s_{276} = T_{274} e(RY_1) \bmod pg(s)$ $s_{277} = T_{275} e(RY_2) \bmod pg(s)$ $s_{278} = T_{276} e(RX_1) \bmod pg(s)$ $s_{279} = T_{277} e(RX_2) \bmod pg(s)$ $s_{280} = T_{278} e(RY_1) \bmod pg(s)$ $s_{281} = T_{279} e(RY_2) \bmod pg(s)$ $s_{282} = T_{280} e(RX_1) \bmod pg(s)$ $s_{283} = T_{281} e(RX_2) \bmod pg(s)$ $s_{284} = T_{282} e(RY_1) \bmod pg(s)$ $s_{285} = T_{283} e(RY_2) \bmod pg(s)$ $s_{286} = T_{284} e(RX_1) \bmod pg(s)$ $s_{287} = T_{285} e(RX_2) \bmod pg(s)$ $s_{288} = T_{286} e(RY_1) \bmod pg(s)$ $s_{289} = T_{287} e(RY_2) \bmod pg(s)$ $s_{290} = T_{288} e(RX_1) \bmod pg(s)$ $s_{291} = T_{289} e(RX_2) \bmod pg(s)$ $s_{292} = T_{290} e(RY_1) \bmod pg(s)$ $s_{293} = T_{291} e(RY_2) \bmod pg(s)$ $s_{294} = T_{292} e(RX_1) \bmod pg(s)$ $s_{295} = T_{293} e(RX_2) \bmod pg(s)$ $s_{296} = T_{294} e(RY_1) \bmod pg(s)$ $s_{297} = T_{295} e(RY_2) \bmod pg(s)$ $s_{298} = T_{296} e(RX_1) \bmod pg(s)$ $s_{299} = T_{297} e(RX_2) \bmod pg(s)$ $s_{300} = T_{298} e(RY_1) \bmod pg(s)$ $s_{301} = T_{299} e(RY_2) \bmod pg(s)$ $s_{302} = T_{300} e(RX_1) \bmod pg(s)$ $s_{303} = T_{301} e(RX_2) \bmod pg(s)$ $s_{304} = T_{302} e(RY_1) \bmod pg(s)$ $s_{305} = T_{303} e(RY_2) \bmod pg(s)$ $s_{306} = T_{304} e(RX_1) \bmod pg(s)$ $s_{307} = T_{305} e(RX_2) \bmod pg(s)$ $s_{308} = T_{306} e(RY_1) \bmod pg(s)$ $s_{309} = T_{307} e(RY_2) \bmod pg(s)$ $s_{310} = T_{308} e(RX_1) \bmod pg(s)$ $s_{311} = T_{309} e(RX_2) \bmod pg(s)$ $s_{312} = T_{310} e(RY_1) \bmod pg(s)$ $s_{313} = T_{311} e(RY_2) \bmod pg(s)$ $s_{314} = T_{312} e(RX_1) \bmod pg(s)$ $s_{315} = T_{313} e(RX_2) \bmod pg(s)$ $s_{316} = T_{314} e(RY_1) \bmod pg(s)$ $s_{317} = T_{315} e(RY_2) \bmod pg(s)$ $s_{318} = T_{316} e(RX_1) \bmod pg(s)$ $s_{319} = T_{317} e(RX_2) \bmod pg(s)$ $s_{320} = T_{318} e(RY_1) \bmod pg(s)$ $s_{321} = T_{319} e(RY_2) \bmod pg(s)$ $s_{322} = T_{320} e(RX_1) \bmod pg(s)$ $s_{323} = T_{321} e(RX_2) \bmod pg(s)$ $s_{324} = T_{322} e(RY_1) \bmod pg(s)$ $s_{325} = T_{323} e(RY_2) \bmod pg(s)$ $s_{326} = T_{324} e(RX_1) \bmod pg(s)$ $s_{327} = T_{325} e(RX_2) \bmod pg(s)$ $s_{328} = T_{326} e(RY_1) \bmod pg(s)$ $s_{329} = T_{327} e(RY_2) \bmod pg(s)$ $s_{330} = T_{328} e(RX_1) \bmod pg(s)$ $s_{331} = T_{329} e(RX_2) \bmod pg(s)$ $s_{332} = T_{330} e(RY_1) \bmod pg(s)$ $s_{333} = T_{331} e(RY_2) \bmod pg(s)$ $s_{334} = T_{332} e(RX_1) \bmod pg(s)$ $s_{335} = T_{33$

o other decode person equipments. Other decode person equipments exhibit a distributed secrecy value, recover c_2 and c_3 , and send them to the equipment of P_j .

[0087] The equipment of P_j checks that $Ec_0 = Wc_2QC_3 \bmod p$ is realized, and when not realized, it stops certification. When this is realized, the equipment of P_j calculates $S_0 = d_1 + c_2$ and $z_1 \bmod q$, and sends S_0 and d_0 to other decode person equipments. Other decode person equipments verify that $Q = g_1 d_0 \bmod p$ and $s_0 = T_12Xjc_2 \bmod p$ and $s_0 = T_13Djc_2 \bmod p$ is realized.

[0088] Since a top type is realized only when the equipment of P_j creates D_j correctly, when not realized at least one, it considers verification is failure. From the right (D_1, \dots, D_n), with the secrecy restoration procedure to exponent part, each decode person equipment restores $D = u_1 z \bmod p$, calculates $m = e/D \bmod p$, and decodes Message m .

[0089] The example of a functional configuration of the decode person equipment in an example 2 is shown in drawing 7. The private key of x_1j, x_2j, y_1j, y_2j , and z_j is memorized by memory 21, the open values w_j, g_1, g_2, p , and q etc. are memorized, and since the information further transmitted to the exterior and the information received from the outside are stored temporarily, memory 21 is used. The distributed random-number generation section 22 consists of the secrecy distribution machine 23, a distributed secrecy verification machine 24, and a distributed secrecy adder 25; and private key x_1j, x_2j, y_1j, y_2j , and z_j are created by these, and the variance r_j of a random number r is also generated. The Hash Function operation of $c = H(u_1, u_2)$ is performed about the receiving cipher E with the hash vessel 26, and the operation of $V_j = (u_1 x_1 + c y_1 u_2 x_2 + c y_2 j v - 1) r_j \bmod p$ is performed by the exponentiation computing element 27. The secrecy distribution section 31 consists of a secrecy distribution machine 32 and a distributed secrecy verification machine 33, and the secrecy value V_j is distributed by V_{jk} with a threshold [of $2t$] verifiable secrecy variational method. the dispersion which the secrecy restoration procedure to the exponent part of V_k is performed with the exponent part secrecy restoration vessel 34, and uses w_1 of D_1, \dots, D_n as a bottom with the BCH codeword verification vessel 35 -- it is checked that a logarithm is the codeword of a BCH code. The broadcast mold communication link receiver 36, the broadcast mold communication link transmitter 37, the individual communication link receiver 38, and the individual communication link transmitter 39 are formed, and each part is made to carry out a sequential operation further by the control section 41.

[0090] The same number is numbered and shown in the part which corresponds the functional configuration of the decode person equipment used for an example 3 at drawing 8 with drawing 7. By the distributed multiplication means 43, value x_1j' which distributed the product of a random number r and a private key x_1 with the secrecy variational method of threshold t , same value x_2j', y_1j' , and y_2j' are called for. The certification section 44 consists of the random-number generation machine 45, a exponentiation computing element 46, and **** multiplication and an adder 47, and it proves that V_j is as a result of [of $u_1 x_1 j' + c y_1 j' u_2 x_2 j' + c y_2 j' v - r_j \bmod p$] count to other decode persons by zero information certification. Verification under zero information certification procedure is performed by the exponentiation computing element 49 and comparator 51 of the verification section 48.

[0091]

[Effect of the Invention] Since the justification of a cipher is verified by verifying whether the value which carried out the exponentiation of the value of the verification type at the time of the decode in a Cramer-Shoup code with the random number with which everyone of a decode person cannot know that value in this invention is set to 1, even if it exhibits the value which carried out the exponentiation, no information about the value in an original verification type is revealed. By proving to a third party that this value was created correctly by zero information certification, it can prove to a third party that the received cipher does not satisfy the original verification type.

[0092] Furthermore, since the value of the verification type before carrying out a exponentiation is not revealed to all the decode person, either, also when not filling a verification type by performing count of carrying out a exponentiation by random numbers, by cooperation of a total-session person by distributed count, Even if there is an inaccurate person in a decode person, since an aggressor can get no profit, he is the safe decode approach with a threshold to the alternative cipher attack.

[0093] Furthermore, since according to another viewpoint of this invention an inaccurate person is specified and a cipher is verified only using just data by making each decode person prove the justification of a count result by zero information certification, it is possible to verify by the computational complexity proportional to several n of a decode person. Moreover, when a right cipher is received by setting the open value of each decode person's proper that each decode person's count result serves as a codeword of a BCH code, and an addressee verifying first that a count result is a codeword, and performing zero information certification only when it is not a codeword, it is possible to perform efficient count, with traffic stopped.

[0094] Furthermore, when other decode persons compute and exhibit the distributed private key which the inaccurate decode person has in cooperation with the case where an inaccurate person is specified Although it also becomes bored, even if 1/3 or more inaccurate persons exist by enabling it to calculate a right result instead of the inaccurate decode person, as long as it is less than 1/2, it is possible to obtain a right verification result and a decode result.

[Translation done.]

NOTICES *

IPPO and NCIPPI are not responsible for any damages caused by the use of this translation.

This document has been translated by computer. So the translation may not reflect the original precisely.

**** shows the word which can not be translated.

In the drawings, any words are not translated.

TECHNICAL FIELD

Field of the Invention] This invention relates to the cipher verification approach that a decode person verifies the justification of a cipher specially, and its program documentation medium, about the safe code approach that the information about a decode person's private key does not leak, also when the content of a communication link is kept secret when communicating by the electrical-communication system, and the content of decode is exhibited.

[Translation done.]

NOTICES *

PO and NCIPi are not responsible for any damages caused by the use of this translation.

This document has been translated by computer. So the translation may not reflect the original precisely.
 .**** shows the word which can not be translated.
 .In the drawings, any words are not translated.

PRIOR ART

Description of the Prior Art] In a cryptosystem strong against a selection plaintext attack, a decode person verifies that the transmitting person of a cipher knows the original plaintext by a certain approach. A Cramer-Shoup code Paper R.Cramer and V.Shoup:"A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack", Advances in Cryptology-CRYPTO'98 and LNCS 1462, Springer-Verlag, pp.13-25, and 1998. It is the public-key-encryption approach that it can prove that it is strong to an accommodative selection cipher attack under an assumption which is called existence of a general purpose one direction nature Hash Function and the difficulty of a Diffie-Hellman judging problem and which is believed widely. A Cramer-Shoup code is the code approach supposing one person's decode person with one private key corresponding to one public key.

[0003] By the Cramer-Shoup code approach that it is already known in the case of the 1 decode person that it is strong to an accommodative selection cipher attack First, choose the big prime factors p and q so that q may divide $p-1$, and the origin g_1 and g_2 of the subgroup G_q of the order q of a multiplicative group Z_p is used. It is $(x_1, x_2, y_1, y_2, z) \in Z_q^5$ about a private key. A public key is set to $1 \times 1 \times g_2 \times 2 \times 2 \bmod p$ of $X=g_1, y_1 \times g_2$ of $Y=g_2 \bmod p$, and $Z=g_1 \times z \bmod p$. The cipher E over plaintext $m \in G_q$ consists of (u_1, u_2, v, e) , and the cipher created correctly satisfies $u_1 = g_1 r \bmod p$, $u_2 = g_2 r \bmod p$, $c = H(u_1, u_2)$, $v = Xr \times Y \bmod p$, and $e = mZr \bmod p$ to a certain random number r . First, $c = H(u_1, u_2)$ is calculated and it verifies whether a cipher fills verification type $u_1 \times 1 + c \times y_1 \times u_2 \times 2 + c \times y_2 \times 2 \times v \bmod p$, the decode person who received this cipher refuses decode of that cipher, when not filling, when filling, calculates $m = e / u_1 \times z \bmod p$ and gets Plaintext m .

[0004] By the above-mentioned verification type, a decode person can check that the maker of a cipher knows the original plaintext m . Since decode is refused to the unjust cipher with which a verification type is not filled, as for an aggressor, information with useful any is not acquired, either. However, when refusing decode by this cipher verification approach as a result of verification, it is actually difficult to prove the information concerning [that the cipher verified to the third party does not serve as $V! = v \bmod p$ as inaccurate / 2 (mod p) / , i.e., $\sqrt{u_1 \times 1 + c \times y_1 \times u_2 \times 2 + c \times y_2 \times 2 \times v}$, and] V , without leaking information in any way.

[0005] Furthermore, by secrecy distribution distributing a corresponding private key to two or more partial private keys to one public key, and making this hold to two or more decode persons so that it may often be carried out by an ElGamal cryptosystem etc. As opposed to an unjust cipher with which a verification type is not filled in this code decode approach when the decode person of the manpower exceeding a threshold cooperates and it applies the decode with a threshold which enables it to decode a cipher Since the count result V of left part $u_1 \times 1 + c \times y_1 \times u_2 \times 2 + c \times y_2 \times 2 \times v$ of a verification type becomes known to two or more decode persons, when the decode person who conspired with the aggressor exists, information is revealed to an aggressor and the safety to a selection cipher attack cannot be maintained.

[0006] the decode approach with a threshold -- paper V.Shoup and R.Gennaro: "Securing threshold cryptosystems against chosen ciphertext attack", Advances in Cryptology-EUROCRYPT, 98, LNCS 1403, Springer-Verlag, and pp.1- 16 and 1998 It is shown under an assumption called existence of random Oracle that the proposed method is strong to an accommodative selection cipher attack.

[0007] However, an assumption called random Oracle can obtain no guarantee about the safety, when it is very unreal and random Oracle is replaced and used for the Hash Function considered that the usual collision is difficult.

[Translation done.]

NOTICES *

PO and NCIPI are not responsible for any damages caused by the use of this translation.

This document has been translated by computer. So the translation may not reflect the original precisely.

**** shows the word which can not be translated.

In the drawings, any words are not translated.

EFFECT OF THE INVENTION

Effect of the Invention] Since the justification of a cipher is verified by verifying whether the value which carried out the exponentiation of the value of the verification type at the time of the decode in a Cramer-Shoup code with the random number with which everyone of a decode person cannot know that value in this invention is set to 1, even if it exhibits the value which carried out the exponentiation, no information about the value in an original verification type is revealed. By proving to a third party that this value was created correctly by zero information certification, it can prove to a third party that the received cipher does not satisfy the original verification type.

0092] Furthermore, since the value of the verification type before carrying out a exponentiation is not revealed to all the decode person, either, also when not filling a verification type by performing count of carrying out a exponentiation by random numbers, by cooperation of a total-session person by distributed count, Even if there is an inaccurate person in a decode person, since an aggressor can get no profit, he is the safe decode approach with a threshold to the alternative cipher attack.

0093] Furthermore, since according to another viewpoint of this invention an inaccurate person is specified and a cipher is verified only using just data by making each decode person prove the justification of a count result by zero information certification, it is possible to verify by the computational complexity proportional to several n of a decode person. Moreover, when a right cipher is received by setting the open value of each decode person's proper that each decode person's count result serves as a codeword of a BCH code, and an addressee verifying first that a count result is a codeword, and performing zero information certification only when it is not a codeword, it is possible to perform efficient count, with traffic stopped.

0094] Furthermore, when other decode persons compute and exhibit the distributed private key which the inaccurate decode person has in cooperation with the case where an inaccurate person is specified Although it also becomes bored, even if $1/3$ or more inaccurate persons exist by enabling it to calculate a right result instead of the inaccurate decode person, as long as it is less than $1/2$, it is possible to obtain a right verification result and a decode result.

[Translation done.]

* NOTICES *

JPO and NCIPi are not responsible for any
damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

TECHNICAL PROBLEM

[Problem(s) to be Solved by the Invention] In a Cramer-Shoup code, the object of this invention, without leaking the information about the value in a verification type entirely When the justification of a cipher can be verified and it is shown that the value of a verification type is not just When the decode person of further plurality [prove / for a third party] cooperates and verifies that the value is created correctly by zero information certification, even if there is an inaccurate person in a decode person The value of a verification type is to offer the cipher verification approach which is not revealed to a decode person, either, its program documentation medium, and its equipment.

[Translation done.]

NOTICES *

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

This document has been translated by computer. So the translation may not reflect the original precisely.

1. **** shows the word which can not be translated.

2. In the drawings, any words are not translated.

MEANS

Means for Solving the Problem] The exponentiation of the value of the verification type at the time of the decode in a Cramer-Shoup code is carried out with the random number with which everyone of a decode person cannot know the value, and the justification of a cipher is verified by verifying whether the result of having carried out the exponentiation is set to 1. Count of carrying out a exponentiation by these random numbers, by carrying out by cooperation of a total-session person by distributed count Also when not filling a verification type, the value of the verification type before carrying out a exponentiation is revealed to no decode person, and it is got blocked. When not just Since calculated value turns into a value which is not 1 and the exponentiation of the value is carried out by the random numbers, even if the value by which the exponentiation is carried out is shown and it is shown that calculated value is not 1, i.e., are not just, the value in front of the exponentiation is hidden, and there is no possibility that information may leak.

[0010] Setting n persons' decode person to P_1 - P_n , each decode person P_j ($j = 1, 2, \dots, n$) shall have the open value w_j of a proper. (x_1, x_2, y_1, y_2, z) $**Zq$ It distributes with the secrecy variational method of threshold t , and let the secrecy value ($x_2 j$ and $y_1 j, y_2 x_1 j, j, z_j$) corresponding to a value w_j be the decode person's P_j private key.

[0011] Moreover, let $X_j = g_1 x_1 j g_2 x_2 j \bmod p$, $Y_j = g_1 y_1 j g_2 y_2 j \bmod p$, and $Z_j = g_1 z j \bmod p$ (X_j, Y_j, Z_j) be the decode person's P_j public keys. It considers as the public key which uses $1 x_1 g_2 x_2 \bmod p$ of $X = g, 1 y_1 g_2 y_2 \bmod p$ of $Y = g y_2 \bmod p$, and $Z = g_1 z \bmod p$ (X, Y, Z) for encryption. It shall connect by the safe channel between each decode person equipment, and each decode person equipment shall use the broadcast mold channel it is guaranteed to be to receive a content with other all the members' same decode person equipment.

[0012] $E = (u_1, u_2, v, e)$ is made into the cipher of the plaintext m enciphered by the Cramer-Shoup code approach. Decode person equipment performs a distributed random-number generation procedure in cooperation, and the decode person's P_j equipment acquires the secrecy value r_j . Here, r_j is a secrecy value corresponding to the value w_j at the time of distributing random-number $r **Zq$ with the secrecy variational method of threshold t , and is the value which can recover r with a secrecy decode procedure from the secrecy value of $t+1$ piece of arbitration. Moreover, each decode person equipment cannot know the value of r , but r becomes the random integer of under or more $0q$ from the property of a distributed random-number generation procedure.

[0013] The equipment of each decode person P_j who received E calculates $c = H(u_1, u_2)$ and $V_j = (u_1 x_1 j + c y_1 j u_2 x_2 j + c y_2 j v - 1) r_j \bmod p$. Furthermore, V_j is distributed with a with a threshold $[\text{ of } 2t]$ verifiable secrecy variational method, and the secrecy value V_{jk} corresponding to a value w_k ($k = 1, 2, \dots, n, k \neq j$) is transmitted through a channel safe for each decode person's P_k equipment. After receiving V_{jk} from all other decode person equipments, the decode person's P_k equipment transmits V_k to all other decode person equipments through a broadcast mold channel. As for each decode person equipment, each V_k which received verifies using V_{kj} that it is a right value.

[0014] $2t+1$ piece is chosen among the right and checked V_k , and it investigates whether the value V restored with the secrecy restoration procedure to exponent part, i.e., $x_1 k + c y_1 k$, and $x_2 k + c y_2 k$ is equal to 1. If not equal, a secrecy restoration procedure will be similarly repeated in other combination, and if a restoration value is all equal to 1 about no $2t+1$ piece combination, decode will be refused and it will stop.

[0015] the private key restoration procedure as opposed to [when each decode person equipment calculates according to the above-mentioned procedure] the exponent part from the right V_k of the arbitration beyond $2t+1$ piece -- $V = (u_1 x_1 + c y_1 u_2 x_2 + c y_2 v - 1) r \bmod p$ -- V can be restored. here, in cooperation with [V / V makes p law and] 1 -- if it becomes -- Cramer-Shoup -- in cooperation with [the original value of verification type $u_1 x_1 + c y_1 u_2 x_2 + c y_2$ in law] v . On the other hand, when V becomes in cooperation with 1, it is in cooperation with [an original verification type] v or a random number r is 0. However, the probabilities for the random number r generated in the distributed random-number generation procedure to be set to 0 are $1/q$, and since they are small enough, they can be disregarded. Therefore, V can consider in cooperation with [an original verification type] v , when in cooperation with 1.

[0016] Here, it is assumed that there are a maximum of t decode persons who commit injustice. these t persons -- (1) -- it is made for the value V of the verification type to the unjust cipher E to be set to 1 -- (2) -- it can deviate from the above-mentioned procedure for two kinds of the object of $**$ of making it the value V of the verification type to the just cipher E not set to 1 [or] First, in order to make the object of (1) successful, it must be made for the value of V restored from a certain $2t+1$ piece V_k to be set to 1. However, before all decode person equipments including inaccurate person equipment get to know the value of V_k which other decode person equipments take out Since the value of V_k of self-equipment cannot be changed after having to distribute the value of one's V_k by the verifiable secrecy distribution approach and getting to know the value of V_k of other decode person equipments Only when the anticipation about V_k of other decode person equipments comes true, an inaccurate decode person can attain the object of (1). The probabilities for anticipation to come true are $1/q$, and since they are small enough, they can be disregarded. Next, since an inaccurate person is at most t persons and, as for other $2t+1$ person equipments, the right value is transmitted even if inaccurate decode person equipment transmits what kind of unjust value V_k about the case of (2), the whole of at least one kind can take the set which consists of $2t+1$ piece V_k of a right value, and $V = 1$ is restored from such a set.

[0017] Since one value of r which fills $V = (u_1 x_1 + c y_1 u_2 x_2 + c y_2 v - 1) r \bmod p$ to any values of $u_1 x_1 + c y_1 u_2 x_2 + c y_2$ about informational leakage when V is not 1 becomes settled Even if the value of $(u_1 x_1 + c y_1 u_2 x_2 + c y_2 v - 1)$ is randomized by r and shows this randomized value, the value before being randomized by r does not leak, that is, the information about $u_1 x_1 + c y_1 u_2 x_2 + c y_2$ does not leak at all by the above-mentioned verification approach.

[0018] As mentioned above, without leaking the information about a private key entirely, if the decode person who commits injustice

According to this invention is less than [of all decode persons] $1/3$, by cooperation of two or more decode person, it is possible to calculate a verification type equivalent to the verification type of the original Cramer-Shoup code approach, and, therefore, two or more decode person's code decode equipment strong against an accommodative selection cipher attack can be constituted.

[0019] When n decode persons are in the above technique, to n data for verification (V_1, \dots, V_n) received from all decode person equipments, each decode person equipment takes out $2t+1$ piece data, and verifies whether a certain verification type is satisfied. When not satisfied, this verification is performed to all the $2t+1$ piece combination that can be taken to n pieces. Therefore, in not satisfying a verification type, it has the fault that computational complexity increases exponentially, to several n of a decode person.

[0020] According to another viewpoint of this invention, in the code decode approach by two or more decode persons, the cipher verification approach and its program documentation medium of a code strong against the accommodative selection cipher attack which can be recovered even if it can perform count efficiently also to many decode persons and $1/3$ or more decode persons perform injustice are offered. That is, as a means to reduce the computational complexity to the number of decode persons, by making each decode person equipment prove the justification of that result by zero information certification, an inaccurate person is specified and, according to another viewpoint of this invention, a cipher is first verified only using just data. By doing so, it is possible to verify by the computational complexity proportional to several n of a decode person. However, since there is much traffic, when injustice hardly happens, effectiveness is bad [the zero information certification used in this case]. When a right cipher is received by setting the open value of each decode person's proper that the count result of each decode person equipment serves as a codeword of a BCH code, and addressee equipment verifying that a count result is a codeword, and performing zero information certification only when it is not a codeword, it becomes possible to perform efficient count, with traffic stopped.

[0021] If based on this approach, the number of the inaccurate persons who can approve is to t persons who fill $3t+1 > n$, and when a safe system with more high tolerance is desired, it is unsuitable. Moreover, although it also becomes bored when an inaccurate person is less than [$1/3$ or more] $1/2$, and other decode person equipments compute and exhibit the distributed private key which the inaccurate decode person has in cooperation with the case where an inaccurate person is specified as a means, a technical problem is solved by enabling it to calculate a right result instead of the inaccurate decode person.

[0022] The concrete means is as follows. n persons' decode person is set to P_1 - P_n , and the open value w_j of a proper is assigned to each decode person P_j . Threshold t which fills $3 < n$ is defined. (x_1, x_2, y_1, y_2, z) $**Z_q$ It distributes with the secrecy variational method of threshold t , and let the secrecy value (x_2, y_1, y_2, z) corresponding to a value w_j be the decode person's P_j private key.

[0023] Moreover, let $X_j = g^{x_1} g^{x_2} \bmod p$, $Y_j = g^{y_1} g^{y_2} \bmod p$, and $Z_j = g^z \bmod p$ (X_j, Y_j, Z_j) be the decode person's P_j public keys. It considers as the public key which uses $1x_1 g^{2x_2} \bmod p$ of $X = g$, $1y_1 g^{2y_2} \bmod p$ of $Y = g$, and $Z = g^z \bmod p$ (X, Y, Z) for encryption. It shall connect by the safe channel between each decode person equipment, and each decode person equipment shall use the broadcast mold channel it is guaranteed to be to receive a content with other all the members' same decode person equipment.

[0024] $E = (u_1, u_2, v, e)$ is made into the cipher of the plaintext m enciphered by the Cramer-Shoup code approach. Decode person equipment performs a distributed random-number generation procedure in cooperation, and the decode person's P_j equipment acquires the secrecy value r_j . Here, r_j is a secrecy value corresponding to the value w_j at the time of distributing random-number $r **Z_q$ with the secrecy variational method of threshold t , and is the value which can recover r with a secrecy decode procedure from the secrecy value of $t+1$ piece of arbitration. Moreover, each decode person cannot know the value of r , but r becomes the random integer of under or more $0q$ from the property of a distributed random-number generation procedure.

[0025] Next, all decode person equipments cooperate, and perform a distributed multiplication means, and each decode person's P_j equipment obtains secrecy value $x_1j', x_2j', y_1j',$ and y_2j' . Secrecy value x_1j' is a value which distributes the product of a random number r and a private key x_1 with the secrecy variational method of threshold t , and is acquired, and can decode x_1j' to $r - x_1 \pmod{q}$ which $t+1$ person's decode person of arbitration has here. r and $x_2 \pmod{q}$, $r - y_1 \pmod{q}$, and $r - y_2 \pmod{q}$ can be similarly restored from the value of $t+1$ piece of arbitration about secrecy value $x_2j', y_1j',$ and y_2j' , respectively.

[0026] Each decode person P_j equipment which received E calculates $c = H(u_1, u_2)$ and $V_j = u_1 x_1j' + c y_1j' u_2 x_2j' + c y_2j' v - r_j \bmod p$, and transmits V_j to all other decode person equipments through a broadcast mold channel. Next, each decode person equipment checks that the exponent part of (V_1, \dots, V_n) is the codeword of a BCH code. When it becomes clear not the codeword of a BCH code but that it is not right, the exponent part of (V_1, \dots, V_n) each decode person's P_j equipment it proves to other decode persons by zero information certification, without leaking the information concerning [that V_j is as a result of / of $u_1 x_1j' + c y_1j' u_2 x_2j' + c y_2j' v - r_j \bmod p$ / count, and] $x_1j', x_2j', y_1j', y_2j',$ and r_j .

[0027] It considers that the decode person P_j who failed in certification is an inaccurate person, and other decode person equipments recover secrecy value x_1j' of the deviation person who is the inaccurate person, $x_2j', y_1j', y_2j',$ and r_j using secrecy value recovery procedure, and he exhibits the value of the right V_j . The rights (V_1, \dots, V_n) including the value of the exhibited right V_j are obtained. After the exponent part of (V_1, \dots, V_n) checks the right thing and that it is a codeword, the secrecy restoration procedure to exponent part restores a value V . Each decode person equipment investigates whether V is equal to 1, and if not equal, decode will be refused and it will stop.

[0028] If equal, each decode person's P_j equipment will calculate $D_j = u_1 z_j \bmod p$, and will transmit it to all other decode person equipments according to a broadcast mold channel. Each decode person equipment which received D_j verifies the codeword same with having carried out to (V_1, \dots, V_n) to (D_1, \dots, D_n), when injustice is detected, performs zero information certification similarly, specifies an inaccurate person, and it recovers the value of the right D_j using secrecy value recovery procedure.

[0029] From the right (D_1, \dots, D_n), with the secrecy restoration procedure to exponent part, each decode person equipment restores $D = u_1 z \bmod p$, calculates $m = e/D \bmod p$, and decodes Message m . the private key restoration procedure as opposed to [when each decode person equipment calculates according to the above-mentioned procedure] the exponent part from the right V_k of the arbitration beyond $2t+1$ piece -- $V = (u_1 x_1 + c y_1 u_2 x_2 + c y_2 v - 1) r \bmod p$ -- V can be restored. here, in cooperation with [V/V makes p law and] 1 -- if it becomes -- Cramer-Shoup -- in cooperation with [the original value of verification type $u_1 x_1 + c y_1 u_2 x_2 + c y_2$ in law] v . On the other hand, when V becomes in cooperation with 1 , it is in cooperation with [an original verification type] v or a random number r is 0 . However, the probabilities for the random number r generated in the distributed random-number generation procedure to be set to 0 are $1/q$, and since they are small enough, they can be disregarded. Therefore, V can consider in cooperation with [an original verification type] v , when in cooperation with 1 .

[0030] Here, it is assumed that there are a maximum of t decode persons who commit injustice. these t persons -- (1) -- it is made for the value V of the verification type to the unjust cipher E to be set to 1 -- (2) -- it can deviate from the above-mentioned procedure for two kinds of the object of $**$ of making it the value V of the verification type to the just cipher E not set to 1 [or] However, the output of all decode person

equipments can detect the existence, if an unjust value is less than [of the whole] $1/3$ when an unjust value exists since it is verified by codeword inspection of a BCH code. In such a case, since each decode person proves the rightness of an output value by zero information certification, the inaccurate person who outputted the unjust value fails in certification, and is eliminated.

[0031] About informational leakage, when V is not 1, since one value of r which fills $V=(u_1x_1+cy_1u_2x_2+cy_2v-1)r \bmod p$ to any values of $u_1x_1+cy_1u_2x_2+cy_2$ becomes settled, by the above-mentioned verification approach, the information about $u_1x_1+cy_1u_2x_2+cy_2$ does not leak at all. As mentioned above, without leaking the information about a private key entirely, if the decode person who commits injustice according to this invention is less than [of all decode persons] $1/3$, by cooperation of two or more decode person, it is possible to calculate a verification type equivalent to the verification type of the original Cramer-Shoup code approach, and, therefore, two or more decode person's code decode approach strong against an accommodative selection cipher attack can be constituted.

[0032] By computing and exhibiting the distributed private key which codeword inspection of a BCH code is not conducted, but zero information certification is always performed in the above-mentioned means on the other hand, an inaccurate person is specified, other decode persons cooperate, and the inaccurate decode person has. Although it also becomes bored, since a right result is calculable instead of the inaccurate decode person, it can respond to less than $1/2$ inaccurate person (in order to determine by majority that zero information certification is right, one half of decode persons at least must be right).

[0033]

[Embodiment of the Invention] The cipher verification approach which is the first example of this invention is explained to one or less example. The cipher created with cipher implementer equipment 11 as shown in drawing 1 is decoded with decode person equipment 12. If it is not a right cipher, in order to avoid carrying out decode refusal freely with decode person equipment 12, it verifies whether decode refusal is appropriate with verification person equipment 13.

[0034] There shall be the big prime factors p and q now, and q shall divide $p-1$. The origin g_1 and g_2 of G_q is chosen at random. It considers as the public key which uses $x_1, g_2, x_2 \bmod p$ of $X=g$, y_1, g_2 of $Y=g, y_2 \bmod p$, and $Z=g, z \bmod p$ for an encryption procedure. Here, it is $((x_1, x_2, y_1, y_2, z) Z_q^5$. It carries out. The public key shall be exhibited with p, q, g_1 , and g_2 as a open parameter. Moreover, the private key shall be stored on the memory of decode person equipment.

[0035] As shown in drawing 2, after receiving cipher $E=(u_1, u_2, v, e)$ of the plaintext m enciphered by the Cramer-Shoup code approach which used X, Y , and Z as the public key (S1), Decode person equipment generates a random number r (S2), and calculates $c=H(u_1, u_2)$ and $V=(u_1x_1+cy_1u_2x_2+cy_2v-1)r \bmod p$ (S3). If V becomes one, this cipher will be considered as acceptance and (S4) and decode count will be performed (S5).

[0036] If V is not 1, it will consider as a rejection. In order to prove that it is a rejection to a third party, $BC(r)$ is exhibited using bit commitment function $BC()$. There are some which are depended on Pedersen in this bit commitment function. That is, a random number s is generated and it calculates with $BC(r, s)=gr^hs \bmod p$. dispersion of h to which g and h use g as a bottom here -- it is under G_q whose logarithm is strange.

[0037] r which constitutes $BC(r, s)$, x_1 which constitutes public keys X and Y , x_2 , and y_1 and y_2 -- using -- $r \bmod p (u_1x_1+cy_1u_2x_2+cy_2v-1)$ -- it proves to a third party by zero information certification, without leaking the secrecy concerning [that the result of having calculated is V , and] r, x_1, x_2 , and y_1 and y_2 (S6). [then,] The following procedures perform this zero information certification.

[0038] dispersion of h which uses g as a bottom for g and h below -- it considers as the origin of G_q whose logarithm is strange. decode person equipment -- random numbers a, a_1, a_2, b_1 , and b_2 -- Z_q -- choosing -- $R=gr^ha \bmod p, RX_1=Rx_1ha_1 \bmod p, RX_2=Rx_2ha_2 \bmod p, RY_1=Ry_1hb_1 \bmod p, RY_2=Ry_2hb_2 \bmod p$ -- R, RX_1, RX_2, RY_1 , and RY_2 are sent to verification person equipment.

[0039] Furthermore, decode person equipment chooses a random number w_0 from Z_q as random, and is $K=g$ and $L=gw_0 \bmod p$ is sent to verification person equipment. Verification person equipment calculates $B=Ke_0Le_1 \bmod p$ by choosing e_0 and e_1 from Z_q as random, and sends B to decode person equipment.

[0040] Decode person equipment chooses random numbers w_1-w_{18} from Z_q as random. $T_1=g_1w_1g_2w_2 \bmod p, T_2=g_1w_3g_2w_4 \bmod p, T_3=gw_5gw_6 \bmod p, T_4=Rw_1hw_7 \bmod p, T_5=Rw_2hw_8 \bmod p, T_6=Rw_3hw_9 \bmod p, T_7=Rw_4hw_{10} \bmod p, T_8=Calculate gw_{11}hw_{12} \bmod p, T_9=gw_{13}hw_{14} \bmod p, T_{10}=gw_{15}hw_{16} \bmod p, T_{11}=gw_{17}hw_{18} \bmod p, T_{12}=u_1w_{11}+cw_{15}u_2w_{13}+cw_{17}v-w_5 \bmod p$. It sends to verification person equipment.

[0041] Verification person equipment sends e_0 and e_1 to decode person equipment.

Decode person equipment checks that $B=Ke_0Le_1 \bmod p$ is realized, and when not realized, it stops certification. When this is realized, Decode person equipment is $z_1=w_1+e_0$ and $x_1 \bmod q, z_2=w_2+e_0$ and $x_2 \bmod q, z_3=w_3+e_0$ and $y_1 \bmod q, z_4=w_4+e_0$ and $y_2 \bmod q, z_5=w_5+e_0$ and r . $z_6=w_6+e_0$ and $a \bmod q, z_7=w_7+e_0$ and $a_1 \bmod q, z_8=w_8+e_0$ and $a_2 \bmod q, z_9=w_9+e_0$ and $b_1 \bmod q, z_{10}=w_{10}+e_0$ and $b_2 \bmod q, z_{11}=w_{11}+e_0$ and $r-x_1 \bmod q, z_{12}=w_{12}+e_0 (a-x_1+a_1) \bmod q, z_{13}=w_{13}+e_0, r$, and $x_2 \bmod q, z_{14}=w_{14}+e_0 (a \text{ and } x_2+a_2) \bmod q, z_{15}=w_{15}+e_0$ and $r-y_1 \bmod q, z_{16}=w_{16}+e_0 (a-y_1+b_1) \bmod q, z_{17}=w_{17}+e_0$ and $r-y_2 \bmod q, z_{18}=w_{18}+e_0 (a-y_2+b_2) \bmod q$. It calculates and z_1-z_{18} , and w_0 are sent to verification person equipment.

[0042] Verification person equipment $L=gw_0 \bmod p, z_1g_2z_2=T_1Xe_0 \bmod p, z_3g_2z_4=T_2Ye_0 \bmod p, z_5hz_6=T_3Re_0 \bmod p, z_1hz_7=T_4e_0(RX_1) \bmod p, z_2hz_8=T_5e_0(RX_2) \bmod p, z_3hz_9=T_6e_0(RY_1) \bmod p, z_4hz_{10}=T_7e_0(RY_2) \bmod p, z_1hz_{12}=T_8e_0(RX_1) \bmod p, z_1hz_{14}=T_9e_0(RX_2) \bmod p$. It verifies that $pgz_{15}hz_{16}=T_{10}(RY_1)e_0 \bmod p, z_1hz_{18}=T_{11}(RY_2)e_0 \bmod p$. It calculates and z_1-z_{18} , and w_0 are sent to verification person equipment.

[0043] The principle of the upper certification is Schnorr. It is the same as that of a signature, and since a verification type is realized only when decode person equipment creates correctly $V, X, Y, R, RX_1, RX_2, RY_1$, and RY_2 , when at least one is not realized, verification is considered as failure.

The second example of this invention is explained to two or less example. As shown in drawing 3 $R > 3$, they are code implementer equipment 11 and 121-12n of each equipment of the decode persons P_1-P_n . It connects with the broadcast mold channel 14, and is 121-12n of decode person equipment. It connects by the channel 15 safe for mutual.

[0044] There shall be the big prime factors p and q now, and q shall divide $p-1$. The origin g_1 and g_2 of G_q is chosen at random. First, n persons' decode person is set to P_1-P_n , and the open value w_j of a proper is assigned to each decode person P_j ($j=1, 2, \dots, n$). Threshold t which fills $3 < t < n$ is defined. All decode person equipments perform the distributed random-number generation procedure of threshold t 3 times, and the decode person's P_j equipment acquires a secrecy value (x_2j and y_1j, y_2x_1j, j, z_j), and makes this the decode person's P_j private key.

Moreover, let $X_j = g_1 x_{1j} g_2 x_{2j} \bmod p$, $Y_j = g_1 y_{1j} g_2 y_{2j} \bmod p$, and $Z_j = g_1 z_j \bmod p$ (X_j , Y_j , Z_j) be the decode person's P_j public keys.

Furthermore, it considers as the public key which uses $1 \times 1 g_2 x_{2j} \bmod p$ of $X = g_1$, $1 y_{1j} g_2 y_{2j} \bmod p$, and $Z = g_1 z_j \bmod p$ for an encryption procedure. Here, it is $((x_1, x_2, y_1, y_2, z) Z_q^5$. It is the random number restored by the secrecy restoration procedure from $t+1$ set of secrecy values ($x_2 j$ and $y_1 j$, $y_2 x_{1j}$, j , z) of arbitration. There is an approach by Pedersen in the distributed random-number generation procedure which generates such a random number. Below, the distributed random-number generation procedure is shown.

[0045] Between each decode person equipment, as shown in drawing 3, there shall be a safe channel 15 and each decode person equipment shall use the broadcast mold channel 14 it is guaranteed to be to receive a content with other all the members' same decode person equipment.

S-1) the equipment of P_j -- two polynomials on Z_q -- $f(X) = a_0 j + a_1 j X + \dots + a_t j X^t$ And $g_j(X) = b_0 j + b_1 j X + \dots + b_t j X^t$ random -- choosing -- every -- $f_j(w_k)$ and $g_j(w_k)$ are transmitted to the equipment except for 1, 2, --, n , and $k=j$ $k=$ -- of P_k through a safe channel.

[0046] S-2) The equipment of P_j calculates $C_{ij} = g_1 a_{ij} g_2 b_{ij} \bmod p$ to $i=1, \dots, t$, and transmits it to all other decode person equipments through a broadcast mold channel.

S-3) The equipment of P_k which received C_{ij} from all other decode person equipments is $g_1 f_j(w_k) g_2 g_j(w_k) = C_0 j w_k$ and $C_1 j w_k$ as $w_k = w_k \bmod q$. -- It verifies that $C_{tj} w_k \bmod p$ is realized.

[0047] S-4) The equipment of P_k is $x_1 k = f_1(w_k) + f_2(w_k) + \dots$ They are $f_n(w_k) \bmod q$ and $x_2 k = g_1(w_k) + g_2(w_k) + \dots$ Distributed random-number value $x_1 k$ and $x_2 k$ are obtained as $+g_n(w_k) \bmod q$.

S-5) $X = C_0, C_1$ -- It is referred to as $C_0 n \bmod p$. Private key $y_1 j$, $y_2 j$, and z_j to which public keys Y and Z and each decode person correspond similarly are also created similarly.

[0048] All decode person equipments generate distributed random-number $r^{**} Z_q$ with a distributed random-number generation procedure, and each decode person's P_j equipment holds the secrecy value r_j (drawing 5, S1). After receiving cipher $E = (u_1, u_2, v, e)$ of the plaintext m enciphered by the Cramer-Shoup code approach which used X , Y , and Z as the public key (S2), each decode person's P_j equipment calculates $c = H(u_1, u_2)$ and $V_j = (u_1 x_{1j} + c y_{1j} u_2 x_{2j} + c y_{2j} v - 1) r_j \bmod p$ (S3).

[0049] Then, the equipment of P_j distributes V_j with a threshold [of $2t$] verifiable secrecy variational method, and the secrecy value V_{jk} corresponding to a value w_k is transmitted through a channel safe for each decode person's P_k equipment (S4). The approach of Pedersen can be used for the verifiable secrecy variational method used here. The following is the procedure.

P-1) g and h which there are the big prime factors P and Q , and Q divides $P-1$, and are made into $Q > p$ are GQ whose value of $\log g h$ is strange. It considers as origin.

[0050] P-2) the equipment of P_j -- ZQ Two upper polynomials $f_j(X) = V_j + a_1 j X + \dots + a_t j X^t$ And $g_j(X) = b_0 j + b_1 j X + \dots + b_t j X^t$ (however, it considers as $a_0 j = V_j$) -- the part of V_j -- removing -- random -- choosing -- every -- $f_j(w_k)$ and $g_j(w_k)$, i.e., V_{jk} , are transmitted to the equipment of P_k through a safe channel.

P-3) The equipment of P_j calculates $C_{ij} = g_1 a_{ij} h b_{ij} \bmod p$ to $i=1, \dots, t$, and transmits it to all other decode person equipments through a broadcast mold channel.

[0051] P-4) The equipment of P_k which received C_{ij} is $g_1 f_j(w_k) h g_j(w_k) = C_0 j w_k$ and $C_1 j w_k$ as $w_k = w_k \bmod q$. -- It verifies that $C_{tj} w_k \bmod p$ is realized, that is, V_{jk} is verified (S5).

P-5) When not realized, the equipment of P_k transmits a "rejection" to all other decode person equipments through a broadcast mold channel.

[0052] When advice of P-6 "a rejection" is $t+1$ or more pieces, it is considered that P_j is an inaccurate person, it is eliminated (S6), and all other decode person equipments discard all the information that the equipment of P_j transmitted before. The step of P-4, and 5 and 6 is the procedure of performing verification of the distributed secrecy value V_{jk} , and an inaccurate person's abatement, and after all decode person equipments finish transmitting data, you may carry out by releasing a rejection list collectively.

[0053] After all decode person equipments distribute V_j with the above-mentioned procedure, each decode person's P_j equipment transmits V_j and $b_0 j$ to all other decode person equipments through a broadcast mold channel (S7). The equipment of each decode person P_j who received this checks that $C_0 j = g_1 V_j h b_0 j \bmod p$ is realized, and verifies V_j (S8). When not realized, like the above, a "rejection" is notified to all other decode person equipments, and an inaccurate person is eliminated (S9).

[0054] $2t+1$ piece is chosen as arbitration from the right and all checked $V_k(s)$ (S10), and it investigates whether the value V restored with the secrecy restoration procedure to exponent part is equal to 1 (S11). The secrecy restoration procedure to exponent part is reference. Cramer, et.al: "A secure and Optimally Efficient Multi-Authority Election Scheme", Advances in Cryptology-Eurocrypt'97, LNCS 1233 Springer-Verlag, pp.103-118, and 1997 It is detailed. The restoration procedure to the exponent part at the time of setting to alpha the set of the index k of $2t+1$ piece V_k chosen as below is shown. The secrecy value of exponent part presupposes that it is the secrecy value acquired with the verifiable secrecy variational method of Pedersen.

[0055] R-1) It is a Lagrange interpolation multiplier first [0056]

[Equation 1]

$$\lambda_{j, \alpha} = \prod_{k \in \alpha, k \neq j} j / (j - k)$$

It calculates by carrying out.

R-2) Next, [0057]

[Equation 2]

$$V = \prod_{j \in \alpha} V_j \lambda_{j, \alpha} \bmod p$$

It calculates. If V is not 1, a secrecy restoration procedure will be similarly repeated in other $2t+1$ piece combination (S12). If a restoration value is all equal to 1 about no combination, a rejection will be notified and it will stop.

[0058] If there is combination set to 1 at least one, this cipher will be considered as acceptance. Each decode person's P_j equipment calculates $D_j = u_1 z_j \bmod p$, as shown in drawing 4 $R > 4$ (S1), and it transmits it to all other decode person equipments according to a broadcast mold channel (S2). the dispersion to which each decode person equipment which received D_j uses u_1 of D_1, \dots, D_n as a bottom -- by checking that a logarithm is the codeword of a BCH code, if it is (S4) and a codeword, the secrecy restoration procedure to the above-mentioned exponent part will restore $D = u_1 z \bmod p$ (S5), $m = e/D \bmod p$ will be calculated, and Message m will be decoded (S6). If it is not a codeword in step S4, what is made to prove the rightness of count and cannot be proved by zero information certification will be discarded as inaccurate D_i (S7).

The third example of this invention is explained to three or less example.

[0059] A safe channel shall be between each decode person equipment, and each decode person equipment shall use the broadcast mold channel it is guaranteed to be to receive a content with other all the members' same decode person equipment. There shall be the big prime factors p and q and q shall divide $p-1$. The origin g_1 and g_2 of G_q is chosen at random. First, n persons' decode person is set to P_1-P_n , and the open value w_j of a proper is assigned to each decode person P_j . Threshold t which fills $3 \leq t \leq n$ is defined.

[0060] First, the secrecy distribution approach by Pedersen is shown. First, g and h It considers as the origin of G_q whose $\log_g h$ is strange. The equipment of the portioner P who distributes the secrecy values a_0 and b_0 is t -th two polynomials $f(X) = a_0 + a_1 X + \dots + a_t X^t$ on Z_q . -- It is $+atX^t$ and $g(X) = b_0 + b_1 X + \dots + b_t X^t$. -- It is $+btX^t$. Except for a_0 , it chooses at random, and $f(w_j)$ and $g(w_j)$ are sent to each addressee's P_j equipment through a safe channel.

[0061] Next, the commitment value E_i of each multiplier is calculated like $E_i = g^{a_i} h^{b_i} \bmod p$ to $i = 0, \dots, t$, and it opens to the public through a broadcast mold channel. Each equipment of P_j which received these is $gf(w_j)$ as $u_{ji} = w_{ji} \bmod q$. $hg(w_j) = E_{0j} E_{1j} \dots E_{tj}$ -- It verifies that $E_{tj} \bmod p$ is realized. This $E_{0j} E_{1j} \dots E_{tj}$ -- The value of $E_{tj} \bmod p$ is called the commitment to the distributed secrecy value of P_j . If the commitment value of each multiplier is exhibited, anyone can also calculate the commitment to which distributed secrecy value of P_j .

[0062] Below, it is $Ped(a_0, b_0)$ about this secrecy distribution approach $[g, h]$. $\rightarrow (a_0, b_0)$ (E_0, \dots, E_t)

** -- it writes like. (a_0, b_0) are confidential information distributed, each equipment of P_j is the distributed secrecy value received through a safe channel, and its (a_0, b_0) are equal to $f(w_j)$ and $g(w_j)$ respectively. (E_0, \dots, E_t) are commitment values of each multiplier exhibited through a broadcast mold channel. $[g, h]$ express the bottom used in case a commitment is created. As long as there is especially no notice about the above-mentioned notation, the multiplier of the polynomial except a constant term shall be chosen at random.

[0063] Thus, from the distributed secrecy value, when polynomial interpolation recovers the original secrecy, the holder of each distributed secrecy value exhibits the value first. It is $g a_0 h b_0 = E_{0j} E_{1j} \dots E_{tj}$ to the exhibited value (a_0, b_0) . -- It checks that $E_{tj} \bmod p$ is realized. The set which that index j makes is set to alpha about $t+1$ (a_0, b_0) of arbitration of which this formula consists. It is a Lagrange interpolation multiplier [0064]

[Equation 3]

$$\lambda_{i, \alpha} = \prod_{k \in \alpha, k \neq i} (i - k) \bmod q$$

It is [0065] when it carries out.

[Equation 4]

$$\sum_{j \in \alpha} \lambda_{i, \alpha} a_0 j \bmod q = a_0$$

A next door and a_0 are recoverable. b_0 is recoverable similarly. The above-mentioned secrecy distribution approach can completely be similarly performed, even if it uses only one bottom. In such a case, it is written as $Ped(a_0) [g] \rightarrow (a_0)$ (E_0, \dots, E_t).

[0066] The random number distributed in cooperation by two or more persons is generable using this secrecy distribution approach. First, the equipment of P_i chooses random numbers a_i and b_i from Z_q , and is this $Ped(a_i, b_i) [g, h] \rightarrow (a_i, b_i)$ (E_{i0}, \dots, E_{it})

** -- it distributes like. All the members of P_1-P_n perform this. Then, the equipment of P_j receives (a_{1j}, b_{1j}) , \dots , (a_{nj}, b_{nj}) from a safe channel, and receives (E_{10}, \dots, E_{1t}) , \dots , (E_{n0}, \dots, E_{nt}) from a broadcast mold channel. At this time, it is the distributed secrecy value (x_{1j}, x_{2j}) of P_j $x_{1j} = a_{1j} + \dots + a_{nj} \bmod q$, $x_{2j} = b_{1j} + \dots + b_{nj} \bmod q$. It is referred to as $+bnj \bmod q$. The random-number value x_1 recovered from this distributed secrecy value is [0067].

[Equation 5]

$$x_1 = \sum_{j \in \alpha} \lambda_{k, \alpha} x_{1j} = a_1 + \dots + a_n \bmod q$$

The value is known by nobody until it comes out, and it is and recovery is performed. Moreover, the commitment value EX_k of the k -th multiplier of the polynomial which makes this secrecy random-number value a constant serves as $EX_k = E_1^k E_2^k \dots E_{nk} \bmod p$. Especially, it is cautious of it being $EX_0 = g^{x_1} h^{x_2} \bmod p$. This approach is called distributed random-number generation, and it is $Rand([a], [b]) [g, h] \rightarrow (a, b)$ (E_0, \dots, E_t).

It writes. $([a], [b])$ is a random-number value generated and means that the value of $[]$ is strange to every calculator. $[g, h]$ -- and $[]$ of semantics $[a], [b]$ (E_0, \dots, E_t) is the same as that of the notation of the above-mentioned secrecy distribution.

[0068] All decode person equipments are the distributed random-number generation procedure of threshold t $Rand([x_1], [x_2]) [g_1, g_2] \rightarrow (x_1, x_2)$ (EX_0, \dots, EX_t)

$Rand([y_1], [y_2]) [g_1, g_2] \rightarrow (y_1, y_2)$ (EY_0, \dots, EY_t)

$Rand([z_1]) [g_1] \rightarrow (z_1)$ (EZ_0, \dots, EZ_t)

** -- performing 3 times like, the decode person P_j acquires a secrecy value $(x_2, y_1, y_2, x_1, j, z_j)$, and makes this the decode person's P_j private key. Moreover, let $X_j = g^{x_1} h^{x_2} \bmod p$, $Y_j = g^{y_1} h^{y_2} \bmod p$, and $Z_j = g^{z_j} \bmod p$ (X_j, Y_j, Z_j) be the decode person's P_j public keys. Furthermore, it considers as the public key which uses $X = EX_0 = g^{x_1} h^{x_2} \bmod p$, $Y = EY_0 = g^{y_1} h^{y_2} \bmod p$, and $Z = EZ_0 = g^{z_1} \bmod p$ for an encryption procedure. It is (x_1, x_2, y_1, y_2, z) Z_q^5 here. It is the random number restored by the secrecy restoration procedure from $t+1$ set of secrecy values $(x_2, y_1, y_2, x_1, j, z_j)$ of arbitration.

[0069] All decode person equipments perform distributed random-number generation procedure $Rand([r], [s]) [g_1, g_2] \rightarrow (r, s)$ (R_0, \dots, R_t), and generate distributed random-number $r^{**} Z_q$, and each decode person's P_j equipment holds the secrecy values r_j and s_j (drawing 6, S1). R is set to $R = R_0 = g^{r_1} h^{s_1} \bmod p$ here.

[0070] Next, all decode person equipments obtain secrecy value $x_1', x_2', y_1',$ and y_2' with a distributed multiplication means (S_2). Secrecy value x_1' is a value which distributes the product of a random number r and a private key x_1 with the secrecy variational method of threshold t , and is acquired, and can decode $rx_1 \bmod q$ here from x_1' which $t+1$ person's decode person of arbitration has. $rx_2 \bmod q$, $ry_1 \bmod q$, and $ry_2 \bmod q$ can be similarly restored from the value of $t+1$ piece of arbitration about secrecy value $x_2', y_1',$ and y_2' , respectively. About such a distributed multiplication means, it performs as follows.

[0071] The decode person's P_j equipment is $Ped(x_1, x_2) [g_1, g_2] \rightarrow (x_1, x_2)$ (EX_{j0}, \dots, EX_{jt}).

It performs. Each equipment of P_j calculates $R_j = g^{r_j} h^{s_j} \bmod p$. This value R_j is $R_j = R_{0j} E_{1j}$ as $u_{ji} = w_{ji} \bmod q$. -- Since you may calculate

like $R_{tj} \bmod p$, it is cautious of the ability of anyone to calculate.

[0072] Next, the polynomial used for distributing x_{1j} and x_{2j} by $Ped(x_{1j}, x_{2j})$ is used for the equipment of P_j as it is, and it is $Ped(x_{1j}, s_{1j})$ $R_j, g_2] \rightarrow (x_{1j}, s_{1j})$ (ERX 1j0, --, ERX1jt).

$Ped(x_{2j}, s_{2j}) [R_j, g_2] \rightarrow (x_{1j}, s_{2j})$ (ERX 2j0, --, ERX2jt)

t performs. However, s_{1j} and s_{2j} also choose at random the polynomial which chooses at random and makes these a constant term.

[0073] To the last, the equipment of P_j is $Ped(x_{1j-rj}, x_{1j-sj+s_{1j}}) [g_1, g_2] \rightarrow (x_{1j}, s_{1j})$ (ERX 1j0, --, ERX1jt).

$Ped(x_{2j-rj}, x_{2j-sj+s_{2j}}) [g_1, g_2] \rightarrow (x_{2j}, s_{2j})$ (ERX 2j0, --, ERX2jt)

t carries out.

[0074] Each equipment of P_1-P_n performs the above-mentioned procedure. The equipment of P_i is the set $(x_{11i}, \dots, x_{1ni})$ of a distributed secrecy value which received to a Lagrange interpolation multiplier [0075]

[Equation 6]

$\lambda_{j, \alpha} = \prod_{k \in \alpha, k \neq j} j/(j-k)$ として、

$$x_{1j}' = \sum_{j \in \alpha} \lambda_{j, \alpha} r_{x1ji} \bmod q$$

It calculates. The set of the index of right x_{1j}' is set to β , and it is [0076] at the time of $|\beta| \geq t+1$.

[Equation 7]

$$\sum_{j \in \beta} \lambda_{j, \beta} x_{1j}' = \sum_{j \in \beta} \{ \lambda_{j, \beta} \sum_{i \in \alpha} \lambda_{i, \alpha} r_{x1ji} \}$$

$$= \sum_{i \in \alpha} \lambda_{i, \alpha} \{ \sum_{j \in \beta} \lambda_{j, \beta} r_{x1ji} \}$$

$$= \sum_{i \in \alpha} \lambda_{i, \alpha} r_{xi} \cdot x_{1i} = r \cdot x_1$$

Since a next door and multiplication result $r \cdot x_1$ are recoverable, it turns out that x_{1j}' is the t -th distributed secrecy value of $r \cdot x_1$. x_{2j}' as well as x_{1j}' is calculated. Furthermore, a distributed multiplication procedure is similarly performed and calculated about secrecy value y_{1j}' and y_{2j}' .

[0077] After receiving cipher $E = (u_1, u_2, v, e)$ to the plaintext m enciphered by the Cramer-Shoup code approach (S3), each decode person's P_j equipment $c = H(u_1, u_2)$ and $V_j = u_1 x_{1j}' + c y_{1j}' u_2 x_{2j}' + c y_{2j}' v - r_j \bmod p$ are calculated, and V_j is transmitted to all other decode person equipments through (S4) and a broadcast mold channel (S5). Next, as for each decode person equipment, the exponent part of (V_1, \dots, V_n) checks that it is the codeword of a BCH code (S6). A codeword verification procedure reference F.J.MacWilliams: "The Theory of Error Correcting Codes", North-Holland Mathematical Library, and pp.201-202 -- or M. Ben-Or and S.Goldwasser, A. Wigerson: "Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation" and 20 th ACM Symposium on Theory of Computing, pp.1-10, and 1988. A codeword verification procedure is shown below.

- $w! = 1$ is used as the n -th root of 1 in $\bmod q$, and it is referred to as $x_{iij} = w_j (i-1) \bmod q$.

- It is [0078] about $j = 1, \dots, \text{all } 2t_j$.

[Equation 8]

$$V_1 x_{11} V_2 x_{22} \dots V_n x_{nn} \bmod p = 1$$

It checks becoming. When it becomes clear with the above-mentioned procedure that the exponent part of (V_1, \dots, V_n) is not right, each decode person's P_j equipment It proves to other decode person equipments by zero information certification, without leaking the information concerning [that V_j is as a result of / of $u_1 x_{1j}' + c y_{1j}' u_2 x_{2j}' + c y_{2j}' v - r_j \bmod p$ / count, and $x_{1j}', x_{2j}', y_{1j}', y_{2j}'$, and r_j (S7).

[0079] This zero information certification is performed as follows. However, by explanation of the procedure to following P_j , since Subscript j is attached to all variables, this is excluded and explained. First, distributed secrecy value x_1' which P_j holds, x_2' , y_1' , y_2' , and r are received. a, a_1, a_2 , and b_1 as a certain random number $R = g_1 r \bmod p$, $RX_1 = ERX_{10} = R x_1 g_2 a_1 \bmod p$, $RX_2 = ERX_{20} = R x_2 g_2 a_2 \bmod p$, $RY_1 = ERY_{10} = R y_1 g_2 b_1 \bmod p$, $RY_2 = ERY_{20} = R y_2 g_2 b_2 \bmod p$. The values R, RX_1, RX_2, RY_1 , and RY_2 of a commitment p becoming can be acquired from the commitment value of the multiplier exhibited with the distributed random-number generation means and the distributed multiplication means to anyone.

[0080] P_j chooses a random number w_0 from Z_q as random, and sends $K = g$ and $L = g w_0 \bmod p$ to other decode person equipments. Other decode person equipments cooperate and are $\text{Rand}([e_0], [e_1]) [K, L] \rightarrow (e_0i, e_1i)$ (Ee_0, \dots, Ee_t).

It performs and $Ee_0 = K e_0 L e_1 \bmod p$ is sent to the equipment of P_j .

[0081] The equipment of P_j chooses random numbers w_1-w_{18} from Z_q as random. $T_1 = g_1 w_1 g_2 w_2 \bmod p$, $T_2 = g_1 w_3 g_2 w_4 \bmod p$, $T_3 = g_1 w_5 g_2 w_6 \bmod p$, $T_4 = R w_1 h w_7 \bmod p$, $T_5 = R w_2 h w_8 \bmod p$, $T_6 = R w_3 h w_9 \bmod p$, $T_7 = R w_4 h w_{10} \bmod p$, $T_8 = \text{Calculate } g w_{11} h w_{12} \bmod p$, $T_9 = g w_{13} h w_{14} \bmod p$, $T_{10} = g w_{15} h w_{16} \bmod p$, $T_{11} = g w_{17} h w_{18} \bmod p$, $T_{12} = u_1 w_{11} + c w_{15} u_2 w_{13} + c w_{17} v - w_5 \bmod p$. It sends to other decode person equipments.

[0082] Other decode person equipments exhibit a distributed secrecy value, recover e_0 and e_1 , and send them to the equipment of P_j . The equipment of P_j checks that $Ee_0 = K e_0 L e_1 \bmod p$ is realized, and when not realized, it stops certification. When this is realized, The equipment of P_j $S_1 = w_1 + e_0$ and $x_1 \bmod q$, $S_2 = w_2 + e_0 \bmod q$, $S_3 = w_3 + e_0 \bmod q$, $S_4 = w_4 + e_0 \bmod q$, $S_5 = w_5 + e_0 \bmod q$, $S_6 = w_6 + e_0 \bmod q$, $S_7 = w_7 + e_0 \bmod q$, $S_8 = w_8 + e_0 \bmod q$, $S_9 = w_9 + e_0 \bmod q$, $S_{10} = w_{10} + e_0 \bmod q$, $S_{11} = w_{11} + e_0 \bmod q$, $S_{12} = w_{12} + e_0 \bmod q$, $S_{13} = w_{13} + e_0 \bmod q$, $S_{14} = w_{14} + e_0 \bmod q$, $S_{15} = w_{15} + e_0 \bmod q$, $S_{16} = w_{16} + e_0 \bmod q$, $S_{17} = w_{17} + e_0 \bmod q$, $S_{18} = w_{18} + e_0 \bmod q$ is calculated, and S_1-S_{18} , and w_0 are sent to other decode person equipments. Other decode person equipments $L = g w_0 \bmod p$, S_1 of $pg(s)$, S_2 of $s_2 = T_1 X e_0 \bmod pg(s)$, S_3 of $s_3 = T_2 Y e_0 \bmod pg(s)$, S_4 of $s_4 = T_3 R e_0 \bmod pg(s)$, S_5 of $s_5 = T_4 R e_0 \bmod pg(s)$, S_6 of $s_6 = T_5 R e_0 \bmod pg(s)$, S_7 of $s_7 = T_6 R e_0 \bmod pg(s)$, S_8 of $s_8 = T_7 R e_0 \bmod pg(s)$, S_9 of $s_9 = T_8 R e_0 \bmod pg(s)$, S_{10} of $s_{10} = T_9 R e_0 \bmod pg(s)$, S_{11} of $s_{11} = T_{10} R e_0 \bmod pg(s)$, S_{12} of $s_{12} = T_{11} R e_0 \bmod pg(s)$, S_{13} of $s_{13} = T_{12} R e_0 \bmod pg(s)$, S_{14} of $s_{14} = T_{13} R e_0 \bmod pg(s)$, S_{15} of $s_{15} = T_{14} R e_0 \bmod pg(s)$, S_{16} of $s_{16} = T_{15} R e_0 \bmod pg(s)$, S_{17} of $s_{17} = T_{16} R e_0 \bmod pg(s)$, S_{18} of $s_{18} = T_{17} R e_0 \bmod pg(s)$, S_{19} of $s_{19} = T_{18} R e_0 \bmod pg(s)$, S_{20} of $s_{20} = T_{19} R e_0 \bmod pg(s)$, S_{21} of $s_{21} = T_{20} R e_0 \bmod pg(s)$, S_{22} of $s_{22} = T_{21} R e_0 \bmod pg(s)$, S_{23} of $s_{23} = T_{22} R e_0 \bmod pg(s)$, S_{24} of $s_{24} = T_{23} R e_0 \bmod pg(s)$, S_{25} of $s_{25} = T_{24} R e_0 \bmod pg(s)$, S_{26} of $s_{26} = T_{25} R e_0 \bmod pg(s)$, S_{27} of $s_{27} = T_{26} R e_0 \bmod pg(s)$, S_{28} of $s_{28} = T_{27} R e_0 \bmod pg(s)$, S_{29} of $s_{29} = T_{28} R e_0 \bmod pg(s)$, S_{30} of $s_{30} = T_{29} R e_0 \bmod pg(s)$, S_{31} of $s_{31} = T_{30} R e_0 \bmod pg(s)$, S_{32} of $s_{32} = T_{31} R e_0 \bmod pg(s)$, S_{33} of $s_{33} = T_{32} R e_0 \bmod pg(s)$, S_{34} of $s_{34} = T_{33} R e_0 \bmod pg(s)$, S_{35} of $s_{35} = T_{34} R e_0 \bmod pg(s)$, S_{36} of $s_{36} = T_{35} R e_0 \bmod pg(s)$, S_{37} of $s_{37} = T_{36} R e_0 \bmod pg(s)$, S_{38} of $s_{38} = T_{37} R e_0 \bmod pg(s)$, S_{39} of $s_{39} = T_{38} R e_0 \bmod pg(s)$, S_{40} of $s_{40} = T_{39} R e_0 \bmod pg(s)$, S_{41} of $s_{41} = T_{40} R e_0 \bmod pg(s)$, S_{42} of $s_{42} = T_{41} R e_0 \bmod pg(s)$, S_{43} of $s_{43} = T_{42} R e_0 \bmod pg(s)$, S_{44} of $s_{44} = T_{43} R e_0 \bmod pg(s)$, S_{45} of $s_{45} = T_{44} R e_0 \bmod pg(s)$, S_{46} of $s_{46} = T_{45} R e_0 \bmod pg(s)$, S_{47} of $s_{47} = T_{46} R e_0 \bmod pg(s)$, S_{48} of $s_{48} = T_{47} R e_0 \bmod pg(s)$, S_{49} of $s_{49} = T_{48} R e_0 \bmod pg(s)$, S_{50} of $s_{50} = T_{49} R e_0 \bmod pg(s)$, S_{51} of $s_{51} = T_{50} R e_0 \bmod pg(s)$, S_{52} of $s_{52} = T_{51} R e_0 \bmod pg(s)$, S_{53} of $s_{53} = T_{52} R e_0 \bmod pg(s)$, S_{54} of $s_{54} = T_{53} R e_0 \bmod pg(s)$, S_{55} of $s_{55} = T_{54} R e_0 \bmod pg(s)$, S_{56} of $s_{56} = T_{55} R e_0 \bmod pg(s)$, S_{57} of $s_{57} = T_{56} R e_0 \bmod pg(s)$, S_{58} of $s_{58} = T_{57} R e_0 \bmod pg(s)$, S_{59} of $s_{59} = T_{58} R e_0 \bmod pg(s)$, S_{60} of $s_{60} = T_{59} R e_0 \bmod pg(s)$, S_{61} of $s_{61} = T_{60} R e_0 \bmod pg(s)$, S_{62} of $s_{62} = T_{61} R e_0 \bmod pg(s)$, S_{63} of $s_{63} = T_{62} R e_0 \bmod pg(s)$, S_{64} of $s_{64} = T_{63} R e_0 \bmod pg(s)$, S_{65} of $s_{65} = T_{64} R e_0 \bmod pg(s)$, S_{66} of $s_{66} = T_{65} R e_0 \bmod pg(s)$, S_{67} of $s_{67} = T_{66} R e_0 \bmod pg(s)$, S_{68} of $s_{68} = T_{67} R e_0 \bmod pg(s)$, S_{69} of $s_{69} = T_{68} R e_0 \bmod pg(s)$, S_{70} of $s_{70} = T_{69} R e_0 \bmod pg(s)$, S_{71} of $s_{71} = T_{70} R e_0 \bmod pg(s)$, S_{72} of $s_{72} = T_{71} R e_0 \bmod pg(s)$, S_{73} of $s_{73} = T_{72} R e_0 \bmod pg(s)$, S_{74} of $s_{74} = T_{73} R e_0 \bmod pg(s)$, S_{75} of $s_{75} = T_{74} R e_0 \bmod pg(s)$, S_{76} of $s_{76} = T_{75} R e_0 \bmod pg(s)$, S_{77} of $s_{77} = T_{76} R e_0 \bmod pg(s)$, S_{78} of $s_{78} = T_{77} R e_0 \bmod pg(s)$, S_{79} of $s_{79} = T_{78} R e_0 \bmod pg(s)$, S_{80} of $s_{80} = T_{79} R e_0 \bmod pg(s)$, S_{81} of $s_{81} = T_{80} R e_0 \bmod pg(s)$, S_{82} of $s_{82} = T_{81} R e_0 \bmod pg(s)$, S_{83} of $s_{83} = T_{82} R e_0 \bmod pg(s)$, S_{84} of $s_{84} = T_{83} R e_0 \bmod pg(s)$, S_{85} of $s_{85} = T_{84} R e_0 \bmod pg(s)$, S_{86} of $s_{86} = T_{85} R e_0 \bmod pg(s)$, S_{87} of $s_{87} = T_{86} R e_0 \bmod pg(s)$, S_{88} of $s_{88} = T_{87} R e_0 \bmod pg(s)$, S_{89} of $s_{89} = T_{88} R e_0 \bmod pg(s)$, S_{90} of $s_{90} = T_{89} R e_0 \bmod pg(s)$, S_{91} of $s_{91} = T_{90} R e_0 \bmod pg(s)$, S_{92} of $s_{92} = T_{91} R e_0 \bmod pg(s)$, S_{93} of $s_{93} = T_{92} R e_0 \bmod pg(s)$, S_{94} of $s_{94} = T_{93} R e_0 \bmod pg(s)$, S_{95} of $s_{95} = T_{94} R e_0 \bmod pg(s)$, S_{96} of $s_{96} = T_{95} R e_0 \bmod pg(s)$, S_{97} of $s_{97} = T_{96} R e_0 \bmod pg(s)$, S_{98} of $s_{98} = T_{97} R e_0 \bmod pg(s)$, S_{99} of $s_{99} = T_{98} R e_0 \bmod pg(s)$, S_{100} of $s_{100} = T_{99} R e_0 \bmod pg(s)$, S_{101} of $s_{101} = T_{100} R e_0 \bmod pg(s)$, S_{102} of $s_{102} = T_{101} R e_0 \bmod pg(s)$, S_{103} of $s_{103} = T_{102} R e_0 \bmod pg(s)$, S_{104} of $s_{104} = T_{103} R e_0 \bmod pg(s)$, S_{105} of $s_{105} = T_{104} R e_0 \bmod pg(s)$, S_{106} of $s_{106} = T_{105} R e_0 \bmod pg(s)$, S_{107} of $s_{107} = T_{106} R e_0 \bmod pg(s)$, S_{108} of $s_{108} = T_{107} R e_0 \bmod pg(s)$, S_{109} of $s_{109} = T_{108} R e_0 \bmod pg(s)$, S_{110} of $s_{110} = T_{109} R e_0 \bmod pg(s)$, S_{111} of $s_{111} = T_{110} R e_0 \bmod pg(s)$, S_{112} of $s_{112} = T_{111} R e_0 \bmod pg(s)$, S_{113} of $s_{113} = T_{112} R e_0 \bmod pg(s)$, S_{114} of $s_{114} = T_{113} R e_0 \bmod pg(s)$, S_{115} of $s_{115} = T_{114} R e_0 \bmod pg(s)$, S_{116} of $s_{116} = T_{115} R e_0 \bmod pg(s)$, S_{117} of $s_{117} = T_{116} R e_0 \bmod pg(s)$, S_{118} of $s_{118} = T_{117} R e_0 \bmod pg(s)$, S_{119} of $s_{119} = T_{118} R e_0 \bmod pg(s)$, S_{120} of $s_{120} = T_{119} R e_0 \bmod pg(s)$, S_{121} of $s_{121} = T_{120} R e_0 \bmod pg(s)$, S_{122} of $s_{122} = T_{121} R e_0 \bmod pg(s)$, S_{123} of $s_{123} = T_{122} R e_0 \bmod pg(s)$, S_{124} of $s_{124} = T_{123} R e_0 \bmod pg(s)$, S_{125} of $s_{125} = T_{124} R e_0 \bmod pg(s)$, S_{126} of $s_{126} = T_{125} R e_0 \bmod pg(s)$, S_{127} of $s_{127} = T_{126} R e_0 \bmod pg(s)$, S_{128} of $s_{128} = T_{127} R e_0 \bmod pg(s)$, S_{129} of $s_{129} = T_{128} R e_0 \bmod pg(s)$, S_{130} of $s_{130} = T_{129} R e_0 \bmod pg(s)$, S_{131} of $s_{131} = T_{130} R e_0 \bmod pg(s)$, S_{132} of $s_{132} = T_{131} R e_0 \bmod pg(s)$, S_{133} of $s_{133} = T_{132} R e_0 \bmod pg(s)$, S_{134} of $s_{134} = T_{133} R e_0 \bmod pg(s)$, S_{135} of $s_{135} = T_{134} R e_0 \bmod pg(s)$, S_{136} of $s_{136} = T_{135} R e_0 \bmod pg(s)$, S_{137} of $s_{137} = T_{136} R e_0 \bmod pg(s)$, S_{138} of $s_{138} = T_{137} R e_0 \bmod pg(s)$, S_{139} of $s_{139} = T_{138} R e_0 \bmod pg(s)$, S_{140} of $s_{140} = T_{139} R e_0 \bmod pg(s)$, S_{141} of $s_{141} = T_{140} R e_0 \bmod pg(s)$, S_{142} of $s_{142} = T_{141} R e_0 \bmod pg(s)$, S_{143} of $s_{143} = T_{142} R e_0 \bmod pg(s)$, S_{144} of $s_{144} = T_{143} R e_0 \bmod pg(s)$, S_{145} of $s_{145} = T_{144} R e_0 \bmod pg(s)$, S_{146} of $s_{146} = T_{145} R e_0 \bmod pg(s)$, S_{147} of $s_{147} = T_{146} R e_0 \bmod pg(s)$, S_{148} of $s_{148} = T_{147} R e_0 \bmod pg(s)$, S_{149} of $s_{149} = T_{148} R e_0 \bmod pg(s)$, S_{150} of $s_{150} = T_{149} R e_0 \bmod pg(s)$, S_{151} of $s_{151} = T_{150} R e_0 \bmod pg(s)$, S_{152} of $s_{152} = T_{151} R e_0 \bmod pg(s)$, S_{153} of $s_{153} = T_{152} R e_0 \bmod pg(s)$, S_{154} of $s_{154} = T_{153} R e_0 \bmod pg(s)$, S_{155} of $s_{155} = T_{154} R e_0 \bmod pg(s)$, S_{156} of $s_{156} = T_{155} R e_0 \bmod pg(s)$, S_{157} of $s_{157} = T_{156} R e_0 \bmod pg(s)$, S_{158} of $s_{158} = T_{157} R e_0 \bmod pg(s)$, S_{159} of $s_{159} = T_{158} R e_0 \bmod pg(s)$, S_{160} of $s_{160} = T_{159} R e_0 \bmod pg(s)$, S_{161} of $s_{161} = T_{160} R e_0 \bmod pg(s)$, S_{162} of $s_{162} = T_{161} R e_0 \bmod pg(s)$, S_{163} of $s_{163} = T_{162} R e_0 \bmod pg(s)$, S_{164} of $s_{164} = T_{163} R e_0 \bmod pg(s)$, S_{165} of $s_{165} = T_{164} R e_0 \bmod pg(s)$, S_{166} of $s_{166} = T_{165} R e_0 \bmod pg(s)$, S_{167} of $s_{167} = T_{166} R e_0 \bmod pg(s)$, S_{168} of $s_{168} = T_{167} R e_0 \bmod pg(s)$, S_{169} of $s_{169} = T_{168} R e_0 \bmod pg(s)$, S_{170} of $s_{170} = T_{169} R e_0 \bmod pg(s)$, S_{171} of $s_{171} = T_{170} R e_0 \bmod pg(s)$, S_{172} of $s_{172} = T_{171} R e_0 \bmod pg(s)$, S_{173} of $s_{173} = T_{172} R e_0 \bmod pg(s)$, S_{174} of $s_{174} = T_{173} R e_0 \bmod pg(s)$, S_{175} of $s_{175} = T_{174} R e_0 \bmod pg(s)$, S_{176} of $s_{176} = T_{175} R e_0 \bmod pg(s)$, S_{177} of $s_{177} = T_{176} R e_0 \bmod pg(s)$, S_{178} of $s_{178} = T_{177} R e_0 \bmod pg(s)$, S_{179} of $s_{179} = T_{178} R e_0 \bmod pg(s)$, S_{180} of $s_{180} = T_{179} R e_0 \bmod pg(s)$, S_{181} of $s_{181} = T_{180} R e_0 \bmod pg(s)$, S_{182} of $s_{182} = T_{181} R e_0 \bmod pg(s)$, S_{183} of $s_{183} = T_{182} R e_0 \bmod pg(s)$, S_{184} of $s_{184} = T_{183} R e_0 \bmod pg(s)$, S_{185} of $s_{185} = T_{184} R e_0 \bmod pg(s)$, S_{186} of $s_{186} = T_{185} R e_0 \bmod pg(s)$, S_{187} of $s_{187} = T_{186} R e_0 \bmod pg(s)$, S_{188} of $s_{188} = T_{187} R e_0 \bmod pg(s)$, S_{189} of $s_{189} = T_{188} R e_0 \bmod pg(s)$, S_{190} of $s_{190} = T_{189} R e_0 \bmod pg(s)$, S_{191} of $s_{191} = T_{190} R e_0 \bmod pg(s)$, S_{192} of $s_{192} = T_{191} R e_0 \bmod pg(s)$, S_{193} of $s_{193} = T_{192} R e_0 \bmod pg(s)$, S_{194} of $s_{194} = T_{193} R e_0 \bmod pg(s)$, S_{195} of $s_{195} = T_{194} R e_0 \bmod pg(s)$, S_{196} of $s_{196} = T_{195} R e_0 \bmod pg(s)$, S_{197} of $s_{197} = T_{196} R e_0 \bmod pg(s)$, S_{198} of $s_{198} = T_{197} R e_0 \bmod pg(s)$, S_{199} of $s_{199} = T_{198} R e_0 \bmod pg(s)$, S_{200} of $s_{200} = T_{199} R e_0 \bmod pg(s)$, S_{201} of $s_{201} = T_{200} R e_0 \bmod pg(s)$, S_{202} of $s_{202} = T_{201} R e_0 \bmod pg(s)$, S_{203} of $s_{203} = T_{202} R e_0 \bmod pg(s)$, S_{204} of $s_{204} = T_{203} R e_0 \bmod pg(s)$, S_{205} of $s_{205} = T_{204} R e_0 \bmod pg(s)$, S_{206} of $s_{206} = T_{205} R e_0 \bmod pg(s)$, S_{207} of $s_{207} = T_{206} R e_0 \bmod pg(s)$, S_{208} of $s_{208} = T_{207} R e_0 \bmod pg(s)$, S_{209} of $s_{209} = T_{208} R e_0 \bmod pg(s)$, S_{210} of $s_{210} = T_{209} R e_0 \bmod pg(s)$, S_{211} of $s_{211} = T_{210} R e_0 \bmod pg(s)$, S_{212} of $s_{212} = T_{211} R e_0 \bmod pg(s)$, S_{213} of $s_{213} = T_{212} R e_0 \bmod pg(s)$, S_{214} of $s_{214} = T_{213} R e_0 \bmod pg(s)$, S_{215} of $s_{215} = T_{214} R e_0 \bmod pg(s)$, S_{216} of $s_{216} = T_{215} R e_0 \bmod pg(s)$, S_{217} of $s_{217} = T_{216} R e_0 \bmod pg(s)$, S_{218} of $s_{218} = T_{217} R e_0 \bmod pg(s)$, S_{219} of $s_{219} = T_{218} R e_0 \bmod pg(s)$, S_{220} of $s_{220} = T_{219} R e_0 \bmod pg(s)$, S_{221} of $s_{221} = T_{220} R e_0 \bmod pg(s)$, S_{222} of $s_{222} = T_{221} R e_0 \bmod pg(s)$, S_{223} of $s_{223} = T_{222} R e_0 \bmod pg(s)$, S_{224} of $s_{224} = T_{223} R e_0 \bmod pg(s)$, S_{225} of $s_{225} = T_{224} R e_0 \bmod pg(s)$, S_{226} of $s_{226} = T_{225} R e_0 \bmod pg(s)$, S_{227} of $s_{227} = T_{226} R e_0 \bmod pg(s)$, S_{228} of $s_{228} = T_{227} R e_0 \bmod pg(s)$, S_{229} of $s_{229} = T_{228} R e_0 \bmod pg(s)$, S_{230} of $s_{$

[0083] Since a top type is realized only when the equipment of P_j creates correctly $V, X, Y, R, RX1, RX2, RY1,$ and $RY2$, when not realized at least one, it considers verification as failure (explanation which omitted the subscript "j" above). It considers that the equipment of the decode person P_j who failed in certification is a deviation person, and other decode person equipments recover a deviation person's secrecy value $x1j', x2j', y1j', y2j'$, and rj using secrecy value recovery procedure, and it exhibits the value of the right V_j . About secrecy value recovery procedure here, it is reference, for example. A.Herzberg, et.al : "Proactive secret sharing or:How to cope with perpetual leakage", Advances in Cryptology-CRYPTO'95, LNCS 963, pp.339-352, Springer-Verlag, and 1995 It is detailed. The rights ($V1, \dots, Vn$) including the value of the exhibited right V_j are obtained.

[0084] After the exponent part of ($V1, \dots, Vn$) checks the right thing, the secrecy restoration procedure to exponent part restores a value V . Each decode person equipment investigates whether V is equal to 1, and if not equal, decode will be refused and it will stop (S8). If equal, each decode person's P_j equipment will calculate $Dj = u1zj \bmod p$ like the case of drawing 4. Transmit to all other decode person equipments according to a broadcast mold channel, and each decode person equipment which received Dj verifies the codeword same with having carried out by receiving to ($D1, \dots, Dn$) ($V1, \dots, Vn$). When injustice is detected, zero information certification is performed similarly, a deviation person is specified, and the value of the right Dj is recovered using secrecy value recovery procedure.

[0085] Zero information certification here is performed as follows. The equipment of P_j chooses a random number $d0$ from Zq as random, and sends $W=g1$ and $Q=g1 \cdot d0 \bmod p$ to other decode person equipments. Other decode person equipments cooperate and are $Rand([c2], [c3]) [W, Q] \rightarrow (c2i, c3i) (Ec0, \dots, Ect)$.

It performs and $Ec0=Wc2QC3 \bmod p$ is sent to the equipment of P_j .

[0086] The equipment of P_j chooses random numbers $d1$ and $d2$ from Zq as random, calculates $T12=g1 \cdot d1 \bmod p$, $T13=u1d1 \bmod p$, and sends it to other decode person equipments. Other decode person equipments exhibit a distributed secrecy value, recover $c2$ and $c3$, and send them to the equipment of P_j .

[0087] The equipment of P_j checks that $Ec0=Wc2QC3 \bmod p$ is realized, and when not realized, it stops certification. When this is realized, the equipment of P_j calculates $S0=d1+c2$ and $z1 \bmod q$, and sends $S0$ and $d0$ to other decode person equipments. Other decode person equipments verify that $Q=g1 \cdot d0 \bmod p$, $s0=T12Xjc2 \bmod p$, $u1s0=T13Djc2 \bmod p$ is realized.

[0088] Since a top type is realized only when the equipment of P_j creates Dj correctly, when not realized at least one, it considers verification as failure. From the right ($D1, \dots, Dn$), with the secrecy restoration procedure to exponent part, each decode person equipment restores $D=u1z \bmod p$, calculates $m=e/D \bmod p$, and decodes Message m .

[0089] The example of a functional configuration of the decode person equipment in an example 2 is shown in drawing 7. The private key of $x1j, x2j, y1j, y2j$, and zj is memorized by memory 21, the open values $wj, g1, g2, p$, and q etc. are memorized, and since the information further transmitted to the exterior and the information received from the outside are stored temporarily, memory 21 is used. The distributed random-number generation section 22 consists of the secrecy distribution machine 23, a distributed secrecy verification machine 24, and a distributed secrecy adder 25, and private key $x1j, x2j, y1j, y2j$, and zj are created by these, and the variance rj of a random number r is also generated. The Hash Function operation of $c=H(u1, u2)$ is performed about the receiving cipher E with the hash vessel 26, and the operation of $Vj=(u1x1j+cylju2x2j+cy2jv-1)rj \bmod p$ is performed by the exponentiation computing element 27. The secrecy distribution section 31 consists of a secrecy distribution machine 32 and a distributed secrecy verification machine 33, and the secrecy value Vj is distributed by Vjk with a threshold [of $2t$] verifiable secrecy variational method. the dispersion which the secrecy restoration procedure to the exponent part of Vk is performed with the exponent part secrecy restoration vessel 34, and uses $w1$ of $D1, \dots, Dn$ as a bottom with the BCH codeword verification vessel 35 -- it is checked that a logarithm is the codeword of a BCH code. The broadcast mold communication link receiver 36, the broadcast mold communication link transmitter 37, the individual communication link receiver 38, and the individual communication link transmitter 39 are formed, and each part is made to carry out a sequential operation further by the control section 41.

[0090] The same number is numbered and shown in the part which corresponds the functional configuration of the decode person equipment used for an example 3 at drawing 8 with drawing 7. By the distributed multiplication means 43, value $x1j'$ which distributed the product of a random number r and a private key $x1$ with the secrecy variational method of threshold t , same value $x2j', y1j'$, and $y2j'$ are called for. The certification section 44 consists of the random-number generation machine 45, a exponentiation computing element 46, and **** multiplication and an adder 47, and it proves that Vj is as a result of [of $u1x1j'+cylju2x2j'+cy2j'v-rj \bmod p$] count to other decode persons by zero information certification. Verification under zero information certification procedure is performed by the exponentiation computing element 49 and comparator 51 of the verification section 48.

[Translation done.]

NOTICES *

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

Brief Description of the Drawings]

[Drawing 1] Drawing showing the system configuration of the example 1 of this invention.

[Drawing 2] The flow chart showing the verification operations sequence of the decode person equipment in the example 1 of this invention.

[Drawing 3] Drawing showing the system configuration of the example 2 of this invention.

[Drawing 4] The flow chart showing the decode operations sequence of the decode person's Pi equipment in the example 2 of this invention.

[Drawing 5] The flow chart showing the verification operations sequence of the decode person's Pi equipment in the example 2 of this invention.

[Drawing 6] The flow chart showing the verification operations sequence of the decode person's Pi equipment in the example 3 of this invention.

[Drawing 7] Drawing showing the functional configuration of the decode person equipment in an example 2.

[Drawing 8] Drawing showing the functional configuration of the decode person equipment in an example 3.

[Translation done.]

NOTICES *

IPPO and NCIPPI are not responsible for any damages caused by the use of this translation.

This document has been translated by computer. So the translation may not reflect the original precisely.
**** shows the word which can not be translated.
In the drawings, any words are not translated.

DRAWINGS

Drawing 1]

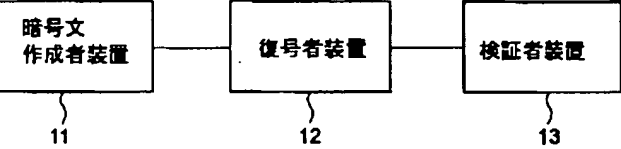


図 1

Drawing 2]

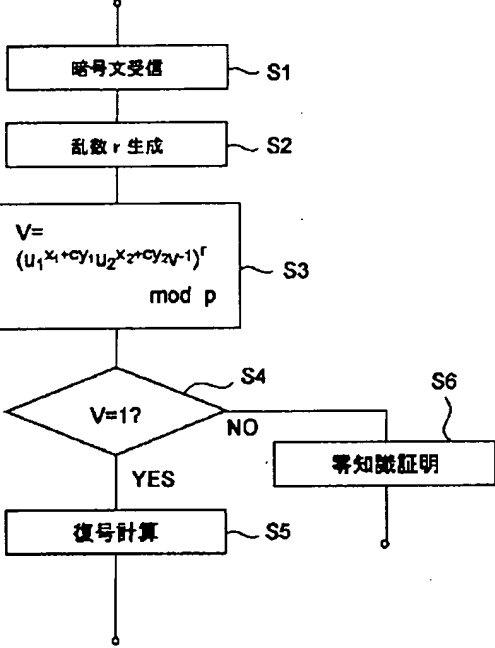


図 2

[Drawing 3]

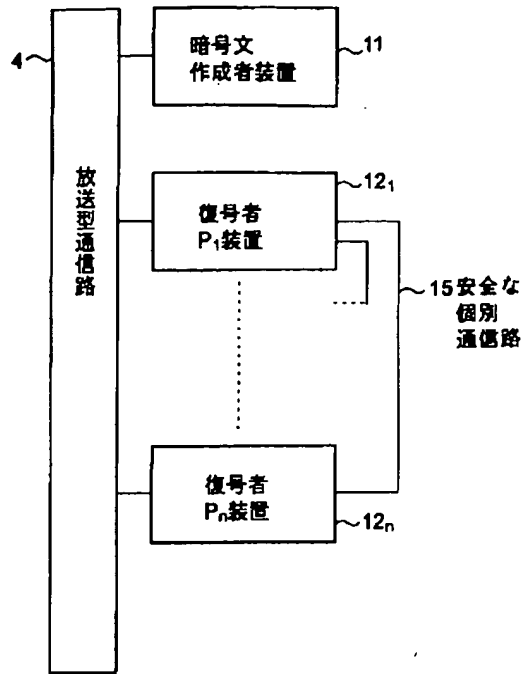


図 3

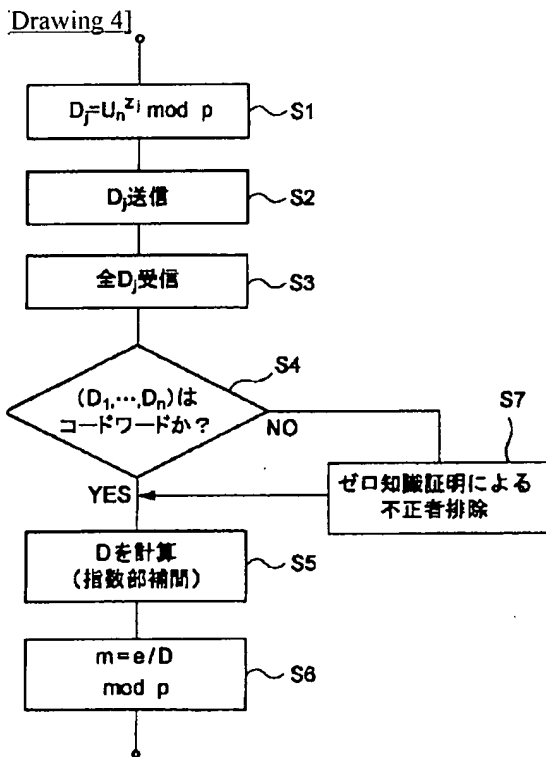


図 4

[Drawing 5]

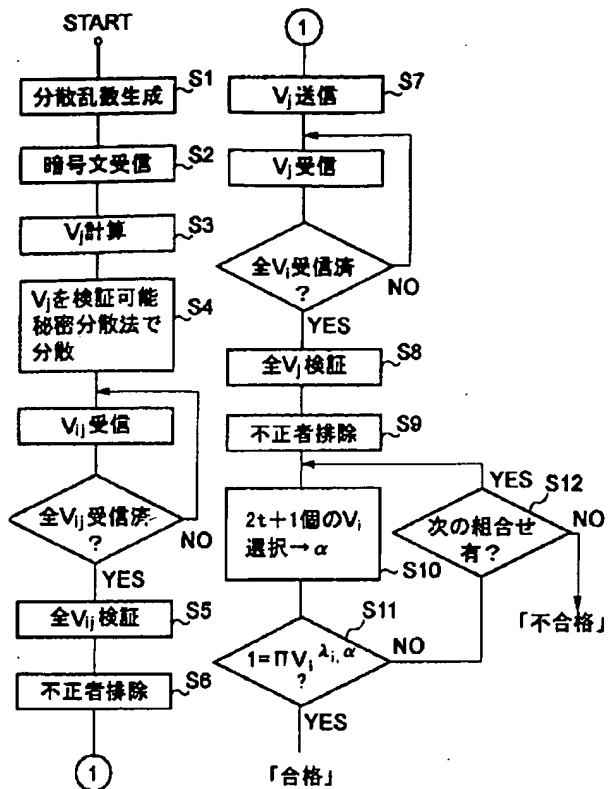


図 5

[Drawing 6]

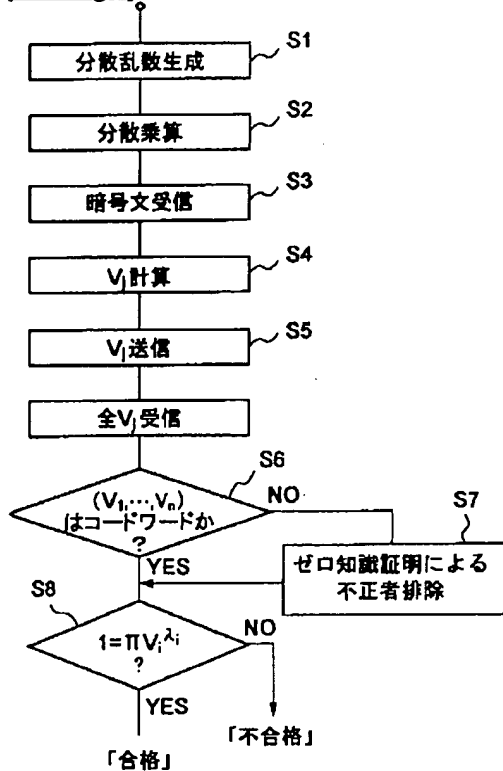


図 6

[Drawing 7]

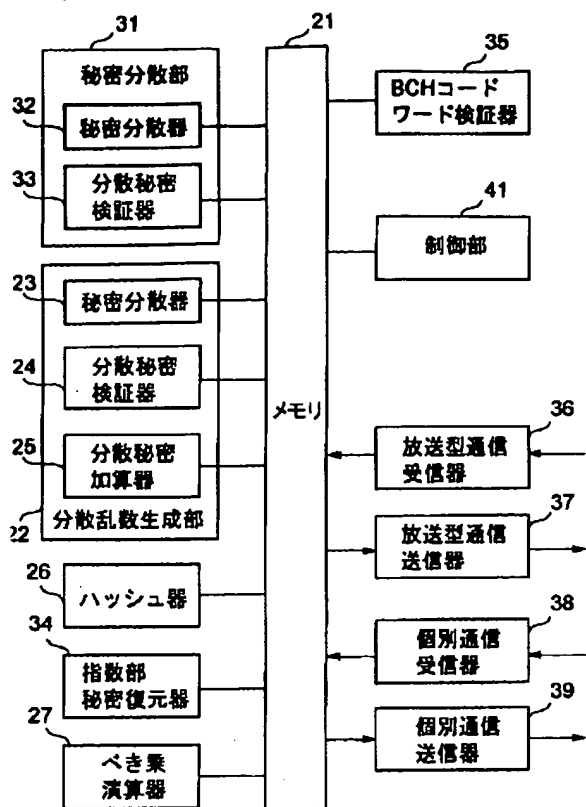


図 7

[Drawing 8]

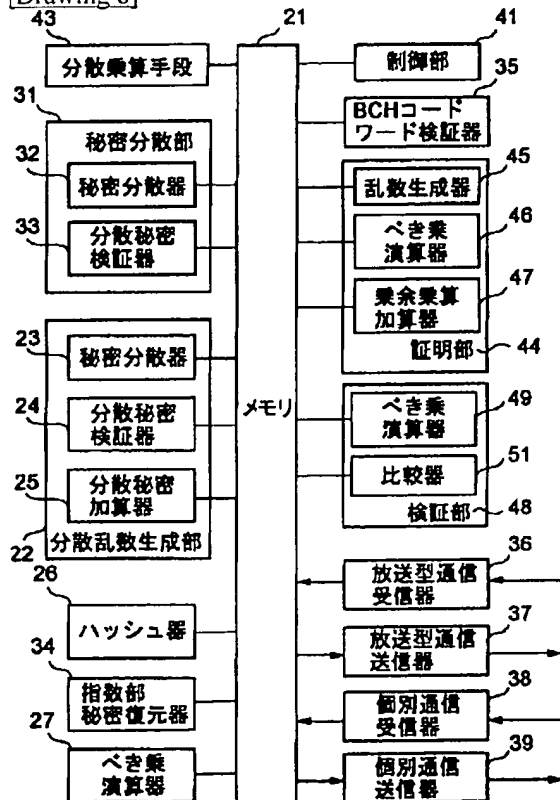


図 8

Translation done.]

THIS PAGE BLANK (USPTO)